MN152128EN

Effective January 2022

Foreseer 7.5.800

Foreseer Server Guide

Table of contents

Introduction

Eaton's Foreseer is an electrical power monitoring system (EPMS) that connects an operation's vast array of devices, regardless of the manufacturer or model. Foreseer facilitates real-time power and environmental system monitoring at a single facility or multiple locations throughout the world, helping organizations reduce power consumption costs and avoid unplanned downtime due to system failure.

- Welcome
- About this Document

Welcome

Foreseer ® is designed to manage your critical site or entire enterprise by monitoring power and environmental inputs from equipment, sensors, and other systems. Monitored points include Meters (analog) and Status (digital) inputs which open a detailed window into the past, present and future performance of your equipment. The unique networked architecture and modular design make Foreseer a cost-effective approach to managing your mission-critical site while maintaining unique analysis and multi-vendor connectivity capabilities. Foreseer is a single integrated system which provides real-time and historical views into the operation of the power and environmental conditions that support your critical operation.

Foreseer is an easy-to-use application consisting of a Server that provides a browser-based interface called WebViews. The Foreseer Server functions as a centralized storage location for information and WebViews acts as a retrieval and display terminal for that information. WebViews allows a User to observe real-time data, respond to events and alarms, as well as graph archived data and project potential failure for every data input. Your system has been pre-configured during installation with equipment, critical data points and other views specific to your operation. The configuration is readily modified to meet changing monitoring needs.

While multiple WebViews clients can access the Server and view its resident data, security functions control who has modification privileges to particular program features. Password authorization can be specified to protect the Foreseer configuration from inadvertent alteration while still allowing its information to be viewed. System Administration controls who has access to select program features by specifying User authorization and overseeing **Server Management**.

Through the Server, the WebViews client offers an enhanced display of up to 20 channel traces in a Historical **Graph** based on the available database. A real-time **Burst Graph** plots values as they are reported while a **ProGraph**™ feature forecasts future performance by extrapolating the data the channel already has archived, allowing you to anticipate adverse conditions before they become serious problems. Authorized Users also can request **Reports** and manage **Alarms** on an individual basis. An integral **Message**

Management feature allows specified personnel to be alerted in the event of certain alarms through a variety of notification services including email.

Foreseer may be equipped with additional software modules specifically designed to enhance its data monitoring and display capabilities. In addition to **Device Drivers**, which provide the interface to each of the monitored devices, the **Simple Network Management Protocol (SNMP) Virtual Agent ™** allows alerts, or traps, to be sent to a specific Network Management Systems (NMS) to report alarms. The WebViews Editor allows authorized users to customize Foreseer WebViews to accurately depict every aspect of the site. Predefined objects can be dragged and dropped in place, user-drawn objects can be animated, and bit mapped images such as pictures and converted AutoCad files can be used as realistic or representative backgrounds for various **WebViews**.

The **Foreseer Server Application** runs under various versions of the Microsoft ® Windows operating systems. See the Release Notes for the latest updates to supported operating systems.

About this Document

Much of the operation of Foreseer should be familiar to those who have used the Microsoft Windows operating system. Foreseer's on-line help facility furnishes more detailed information on program operation. Server assistance is always readily available by selecting the View Help command under the Help Menu. A Help window organizes assistance by Contents, which groups help topics by subject.

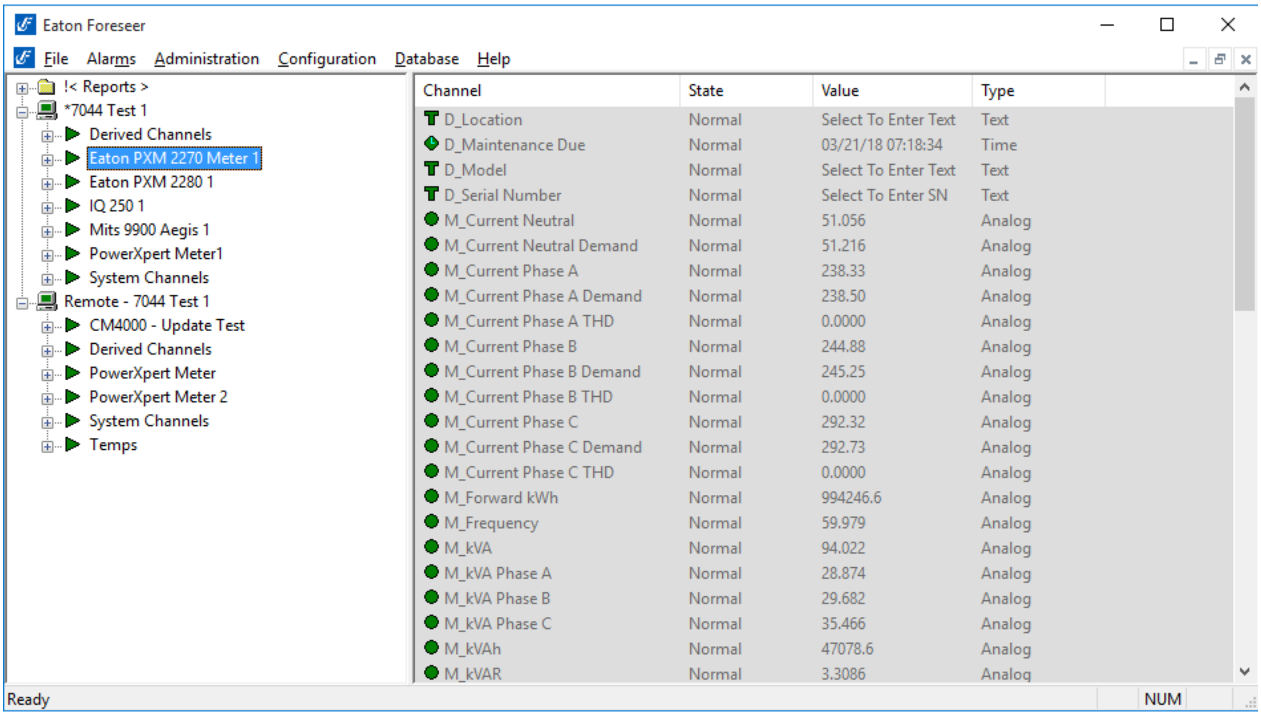
In addition, specific colors are used to identify certain program elements:

Menu Commands
Window Titles
Keyboard Keys
Toolbar Commands
Parameter Fields
Foreseer Features

You can exit on-line assistance at any time simply by closing the **Help** window.

Getting Started

Foreseer is designed to be quick and easy to install and configure. Getting started with Foreseer Server consists of verifying that the Server platform meets minimum system requirements and gathering data on the devices to be monitored.



- !< Reports >
- *7044 Test 1
  - Derived Channels
  - Eaton PXM 2270 Meter 1
  - Eaton PXM 2280 1
  - IQ 250 1
  - Mits 9900 Aegis 1
  - PowerXpert Meter1
  - System Channels
- Remote - 7044 Test 1
  - CM4000 - Update Test
  - Derived Channels
  - PowerXpert Meter
  - PowerXpert Meter 2
  - System Channels
  - Temps

Channel	State	Value	Type
D_Location	Normal	Select To Enter Text	Text
D_Maintenance Due	Normal	03/21/18 07:18:34	Time
D_Model	Normal	Select To Enter Text	Text
D_Serial Number	Normal	Select To Enter SN	Text
M_Current Neutral	Normal	51.056	Analog
M_Current Neutral Demand	Normal	51.216	Analog
M_Current Phase A	Normal	238.33	Analog
M_Current Phase A Demand	Normal	238.50	Analog
M_Current Phase A THD	Normal	0.0000	Analog
M_Current Phase B	Normal	244.88	Analog
M_Current Phase B Demand	Normal	245.25	Analog
M_Current Phase B THD	Normal	0.0000	Analog
M_Current Phase C	Normal	292.32	Analog
M_Current Phase C Demand	Normal	292.73	Analog
M_Current Phase C THD	Normal	0.0000	Analog
M_Forward kWh	Normal	994246.6	Analog
M_Frequency	Normal	59.979	Analog
M_kVA	Normal	94.022	Analog
M_kVA Phase A	Normal	28.874	Analog
M_kVA Phase B	Normal	29.682	Analog
M_kVA Phase C	Normal	35.466	Analog
M_kVAh	Normal	47078.6	Analog
M_kVAR	Normal	3.3086	Analog

- System Requirements
- Supported Environments
- SQL Server Express Installation
- Hardware and Security Considerations
- Security Considerations for Interactive Remote Access
- Recommended Security Guidelines

System Requirements

Foreseer has certain hardware and software requirements; exceeding these prerequisites will enhance the performance of the program. It's essential that you run Foreseer on server class machines. Refer to the Release Notes for the current recommended minimum hardware, operating system, and database requirements.

Minimum Hardware Requirements

To run Foreseer, you will need a server class machine with

- A minimum of two quad-core processors
- 16 GB of RAM
- 100 GB of free drive space.

Supported Environments

Supported Operating Systems

Windows Desktop Operating Systems	Message Manager	Outpost
Windows 10 Professional, x64	X	X
Windows 10 Enterprise, x64	X	X

Windows Server Operating Systems	Server & Message Manager
Windows Server 2012 R2 Std	X
Windows Server 2012 R2 Datacenter	X
Windows Server 2016	X
Windows Server 2019	X

Supported Database Platforms

- SQL Server 2012 Express w/ Advanced Services, Standard, Enterprise, Enterprise Core, SP2
- SQL Server 2014 Express w/ Advanced Services, Standard, Enterprise
- SQL Server 2016 Express w/ Advanced Services, Standard, Enterprise
- SQL Server 2017 Express w/ Advanced Services, Standard, Enterprise
- SQL Server 2019 Express w/ Advanced Services, Standard, Enterprise

Supported Browsers

Please check the Foreseer Release Notes for supported browser information.

SQL Server Express Installation

SQL Server 2016 Express is shipped with Foreseer 7 and installation is straightforward. SQL Server 2016 Express uses .NET 4.6.

Hardware and Security Considerations

Foreseer also has certain hardware and software prerequisites that must be addressed prior to installing the program on the Server. Hardware prerequisites consist of completing the Configuration Checklist for all of the Devices to be monitored, then establishing physical connections between the Server and the Devices to be monitored.

Security Considerations consist of the following best practices:

- Physical access to server hosting Foreseer and the associated system should be restricted, monitored and logged at all times.
- Physical access to the communication lines should be restricted to reduce the risk of intrusion.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.

- Access to physical ports and removable media should be controlled and limited.
- Do not connect unauthorized USB device, CD/DVD or SD card for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB, CD/DVD or SD card slot, scan the device for malware and viruses.
- Foreseer servers should be deployed on systems with limited access to the Internet and less trusted networks. The use of email and other functions not necessary for Foreseer to operate should be limited and protected appropriately.

You should restrict access to ports through the Windows Firewall. Foreseer needs the following ports:

- Port 80 (disabled by default in Apache), required only if you allow HTTP access to WebViews and WebAdmin. HTTP access is inherently insecure and is not recommended.
- Port 81, (disabled by default in the Foreseer web server), required only if you allow unsecured access for Message Manager.
- Port 443, required for HTTPS access for WebViews and WebAdmin.
- Port 444, required for secure access for Message Manager.
- Port 2100, required for Remote/Redundant Foreseer Servers.

SQL Server may require additional ports.

Before proceeding it is recommended that you complete the Configuration Checklist to use as a reference during program installation. Refer to the Installation and Upgrade Guide for a printable copy of the Configuration Checklist.

Security Considerations for Interactive Remote Access

Interactive remote access to Foreseer or third-party communication interfaces should be limited and secured. Windows Remote desktop access should be configured according to the following:

- Only allow log in from specific hosts. You can use white list using the Windows Firewall.
- Use client encryption Network Level Authentication (NLA).
- Limit access to users in a designated remote access group; e.g., create a group in Active Directory and assign users or user.
- Limit access to explicit machines; i.e., white list access.
- Always prompt for client credentials; i.e., do not store credentials.
- Delete temporary folders when session ends.
- Apply account lockout policy (< 30 minutes default).

Recommended Secure Hardening Guidelines

Foreseer is designed with Cybersecurity as an important consideration. A number of Cybersecurity features are now offered in the product which, if implemented as per the recommendations in this section, will minimize Cybersecurity risk. This section provides information and guidelines on how to securely deploy and maintain a Foreseer installation. By following the guidelines provided here within, sites can play a proactive role in minimizing Cybersecurity risks.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys best practices and the latest technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices white papers to its customers that can be referenced at:

Please refer to the Foreseer Recommended Security Hardening Guide (MN152124EN) for the latest information.

http://www.eaton.com/cybersecurity

- Running Foreseer with Minimum Privileges

Running Foreseer Services with Minimum Privileges

In highly secure environments, it may be necessary to run Foreseer using a limited local or domain Windows Authentication account. By default, only privileged user groups such as local and domain administrators can install, stop, start, and restart a Windows service.

The Windows operating system provides an entire suite of command line utilities that can be leveraged to grant users the ability to work with services. The following provides guidance on how to use a reduced user account to run the **Eaton Foreseer** and **Foreseer Apache** services.

The following are scenarios you can follow to reduce the privileges required for an account to run both the Eaton Foreseer service and the Foreseer Apache service.

> ⓘ These scenarios may not work in your environment, and depend on SQL configuration or group policies at your site. Please contact your system administrator for assistance with following these steps. User is an Active Directory User on the System Where Foreseer is Installed

1. Install the Foreseer application, Microsoft SQL Server, and the Eaton Foreseer and Foreseer Apache services as an administrator.
2. Configure a user as a standard user (lowest level apart from Guest which is normally turned off) from both Active Directory and the local system.

3. Open “Services” and go to the properties for both the Eaton Foreseer and Foreseer Apache services.
4. Make sure that the logon for both the services Eaton Foreseer and Foreseer Apache are changed to the standard user account instead of Local System Account
5. Give “Full Control” rights to “Eaton Corporation” (installed folder) to this standard user. This provides write accesses for apache logs, Foreseer logs, Foreseer reports, CSS updates etc.

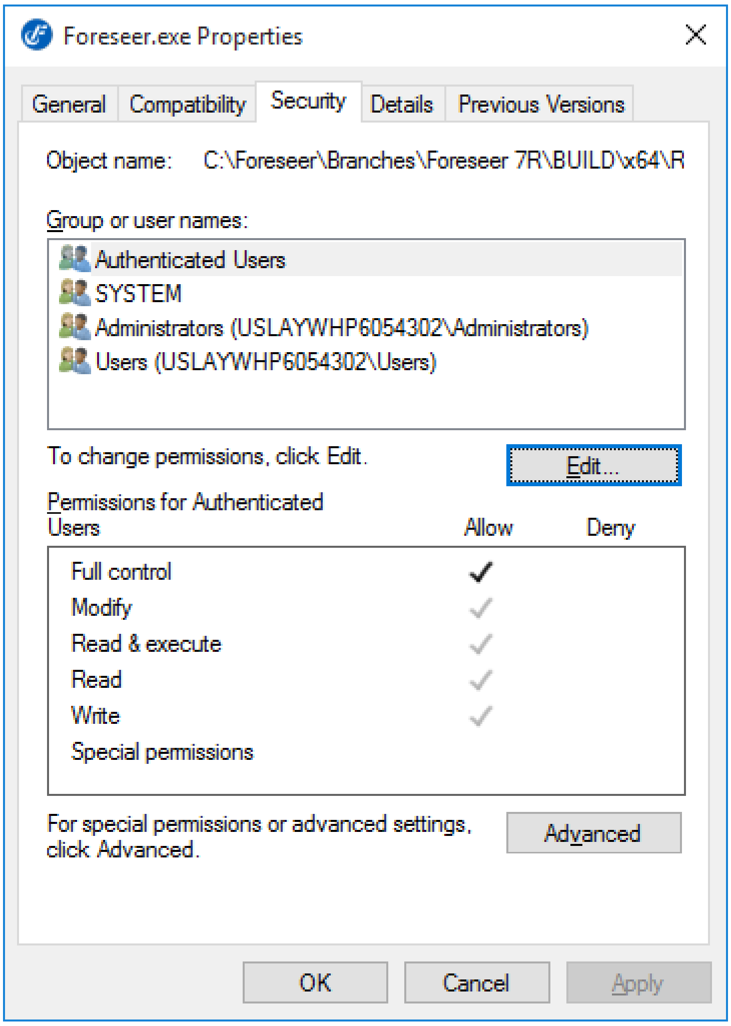
> ⓘ Eaton strongly recommends proper disaster recovery etiquette in the form of timely system backups. Advanced procedures, if not performed correctly, could pose significant risk to a production system. If you are not comfortable with performing this procedure on your own, please contact your IT Administrator for further assistance

- Assigning Full Control Rights to the Foreseer Folder
- Verify Account
- Assign Rights
- Configure Foreseer and Apache Service Log On

Assigning Full Control Rights to the Foreseer Folder

With Foreseer v7 installed on your server, perform the following steps:

1. Navigate to the drive location where you installed Foreseer (typically C:\Eaton Corporation\Foreseer).   Access the Properties of the Foreseer folder.
2. Add the designated user (local or domain) that will run the Foreseer and Apache services. You must provide Full Control rights to this user. If prompted, apply these changes to all sub-folders in the Foreseer directory.



Object name: C:\Foreseer\Branches\Foreseer 7R\BUILD\x64\R

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (USLAYWHP6054302\Administrators)
- Users (USLAYWHP6054302\Users)

Permissions for Authenticated Users	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

3. Click **OK** to apply these changes and make them effective.

Verify Account

Verify account has “Log on as a Service” and “Act as part of the Operating System” access

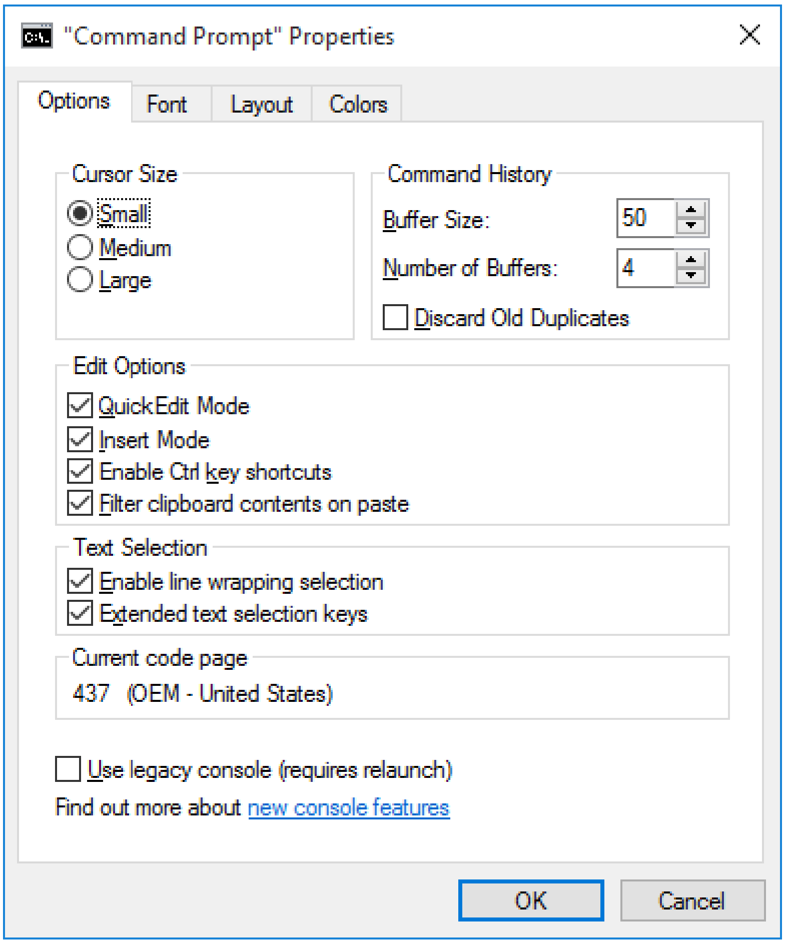
1. Open Administrative Tools and select Local Security Policy from the list
2. Expand Local Policies and click User Rights Assignment
3. From the list in the right-hand pane, right click on *Act as part of the operating system* and select properties
4. Click the Add User or Group... button and add the designated user.
5. Repeat Steps 3 and 4 for the *Log on as a service* policy.

Assign Rights

Assign Rights to Access, Start, Stop, and Restart Services

This process provides guidance on assigning rights to access, start, stop and restart services tied to the Foreseer software platform. This process makes use of the Windows Command Prompt. To copy and paste text for documented procedures configure your

Command Prompt for easy usage. Right click on the title bar and select properties. On the options tab check the Quick-Edit Mode box.



Cursor Size

● Small
○ Medium
○ Large

Command History

Buffer Size: 50

Number of Buffers: 4

□ Discard Old Duplicates

Edit Options

☑ QuickEdit Mode
☑ Insert Mode
☑ Enable Ctrl key shortcuts
☑ Filter clipboard contents on paste

Text Selection

☑ Enable line wrapping selection
☑ Extended text selection keys

Current code page

437 (OEM - United States)

□ Use legacy console (requires relaunch)

Find out more about new console features

You can now use the mouse to highlight the text you want to copy. Once the text is copied, press the Enter key. The text can be pasted to another application like Notepad. To paste text into the command window, right click on the title bar and select Edit>Paste.

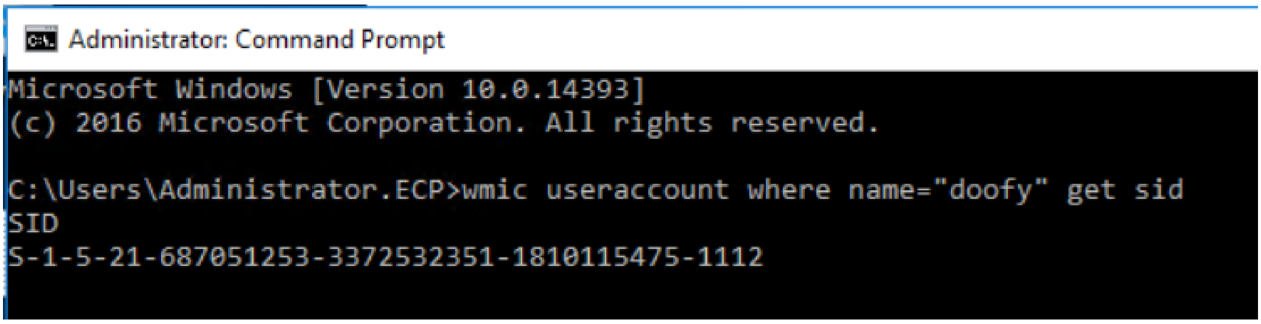
- Part 1 - Retrieve Windows User’s SID
- Part 2 - Granting Access to Windows Service Control Manager
- Part 3 - Granting Access to Eaton Foreseer
- Part 4 - Granting Access to Foreseer Apache

Part 1 - Retrieve Windows User’s SID

Before assigning rights, you must have the SID of the account you wish to user to run the services. You can do this very easily though a Windows Command Prompt using the following command:

wmic useraccount where name='AccountName' get sid

Enter the following command above. Be sure to specify the name of the user account within the double quotes. When you press enter, the SID string will be provided. Copy and paste this into a text file as you will need it for the steps that follow.



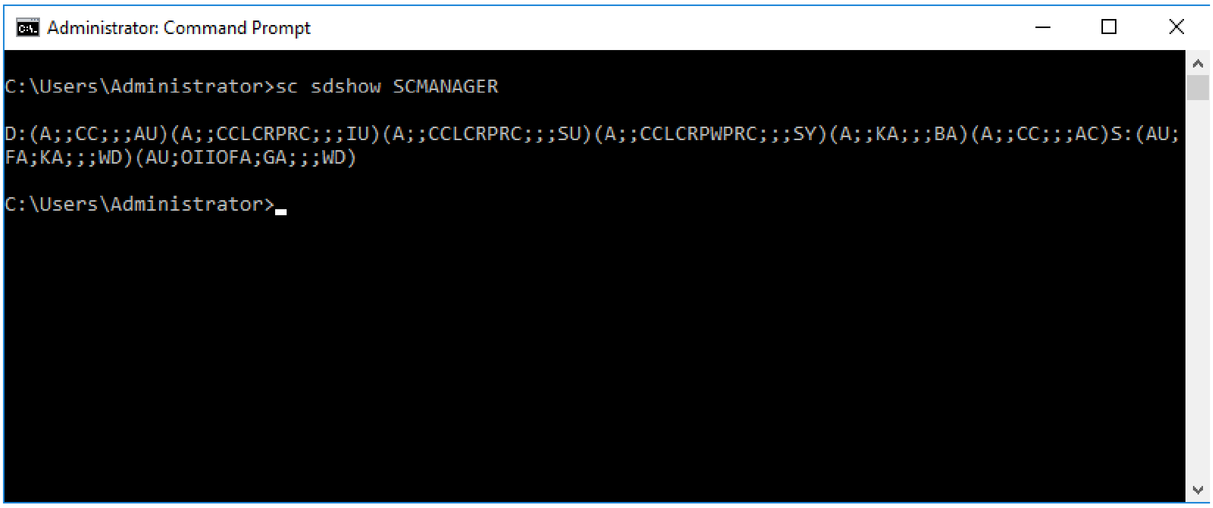
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.ECP>wmic useraccount where name="doofy" get sid
SID
S-1-5-21-687051253-3372532351-1810115475-1112
```

Part 2 - Granting Access to Windows Service Control Manager

The Service Control Manager (SCMANAGER) is used by Windows to operate all interactive services within the operating system.   By default, only local Administrators, domain Administrators, and Power Users have the ability to interact with the Service Control Manager.

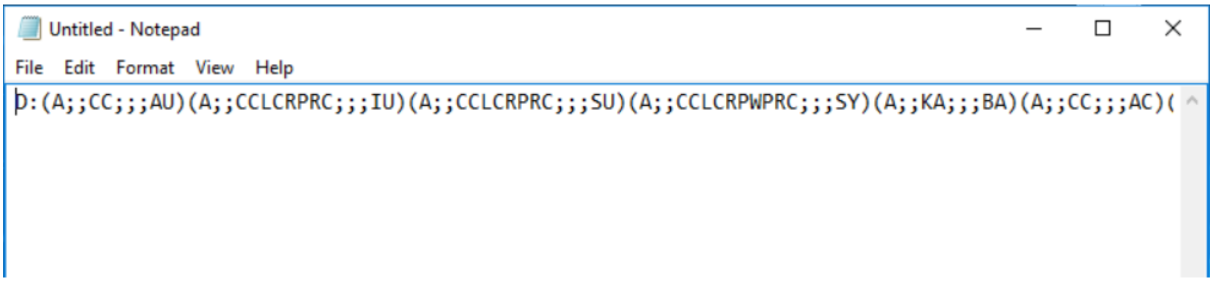
To add your user account, perform the following steps:

1. From a command prompt, run “sc sdshow SCMANAGER”. It will return something like this:



```
C:\Users\Administrator>sc sdshow SCMANAGER

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)S:(AU;
FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

C:\Users\Administrator>
```

2. Copy the entire string and paste into a text editor.

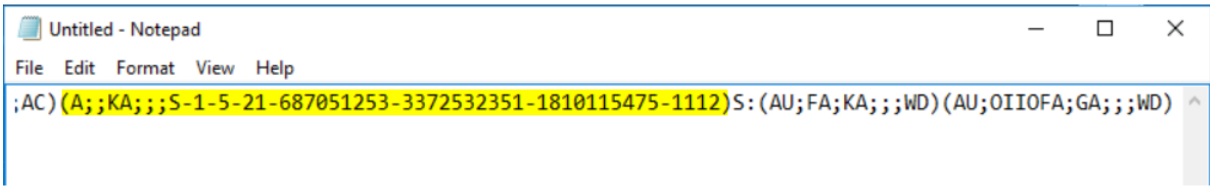


```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(
```

3. Privileges are assigned as a list of parenthetical citation. You will need to add a parenthetical citation to the list that includes the privilege string and SID of your

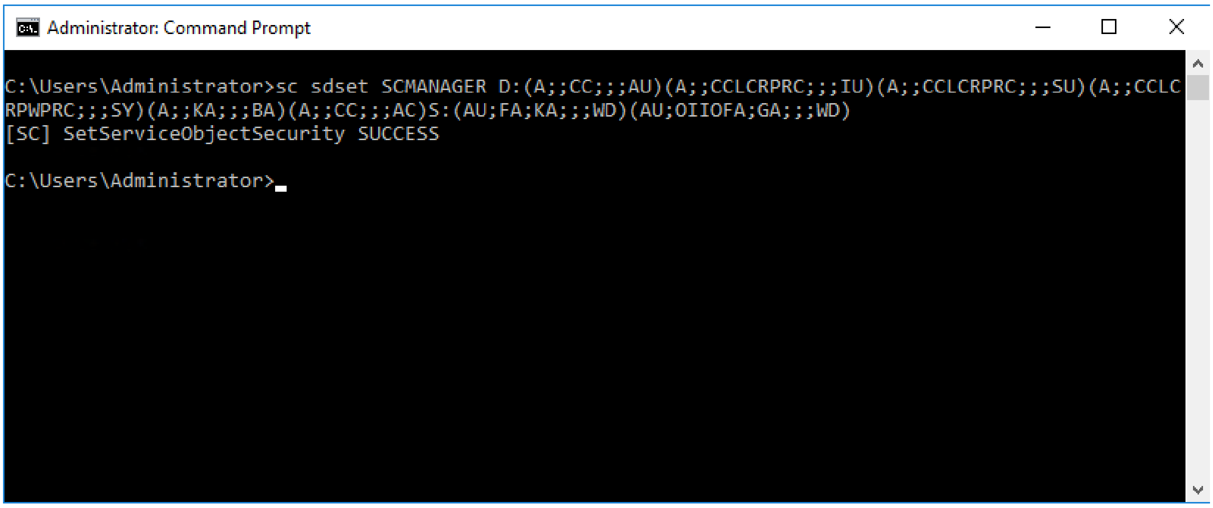
designated user. You must add the citation prior to the “S:” designation. Assigning your user access by adding the following string with USERSID replaced with the actual account SID from Step 1 of this procedure.

(A;;KA;;;USERSID)



```
;AC)(A;;KA;;;S-1-5-21-687051253-3372532351-1810115475-1112)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

4. Finally, copy the entire modified string. At a command prompt, run “sc sdset SCMANAGER <copied string from text editor>”. Press Enter. You will receive a SUCCESS message once the process is complete.

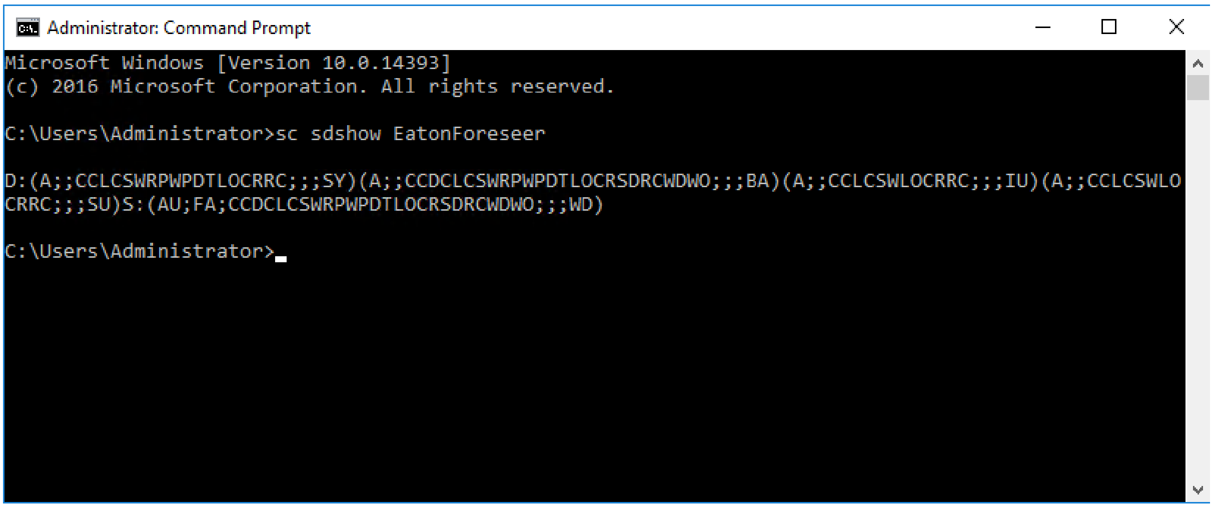


```
C:\Users\Administrator>sc sdset SCMANAGER D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLC
RPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
[SC] SetServiceObjectSecurity SUCCESS

C:\Users\Administrator>
```

Part 3 - Granting Access to Eaton Foreseer

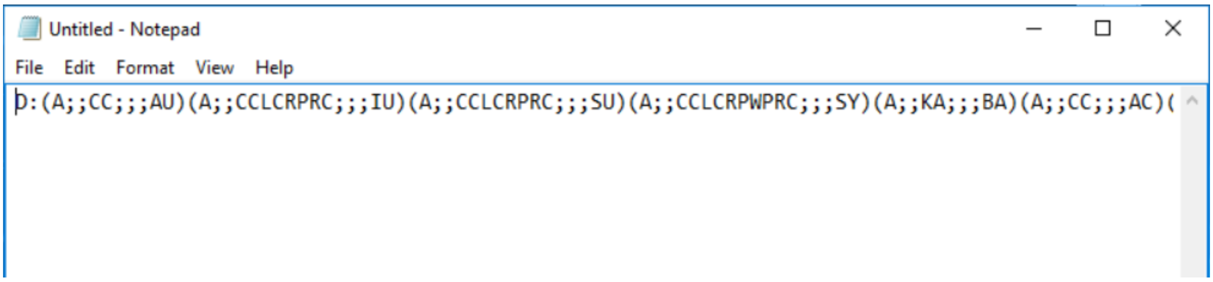
The Foreseer service is the engine of the EPMS software platform. To add your user account, perform the following steps:

1. From a command prompt, run “sc sdshow EatonForeseer”. It will return something like this:



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sc sdshow EatonForeseer

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLO
CRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

C:\Users\Administrator>_
```

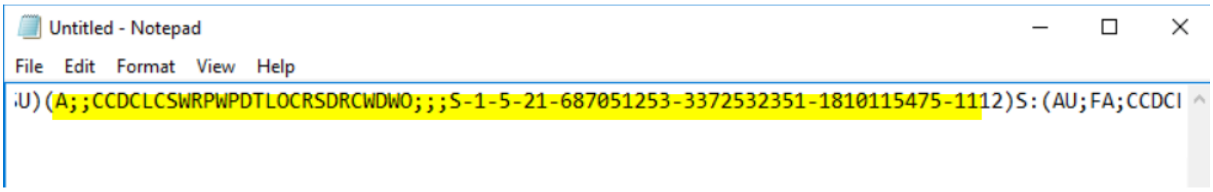
2. Copy the entire string and paste into a text editor.



```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(
```

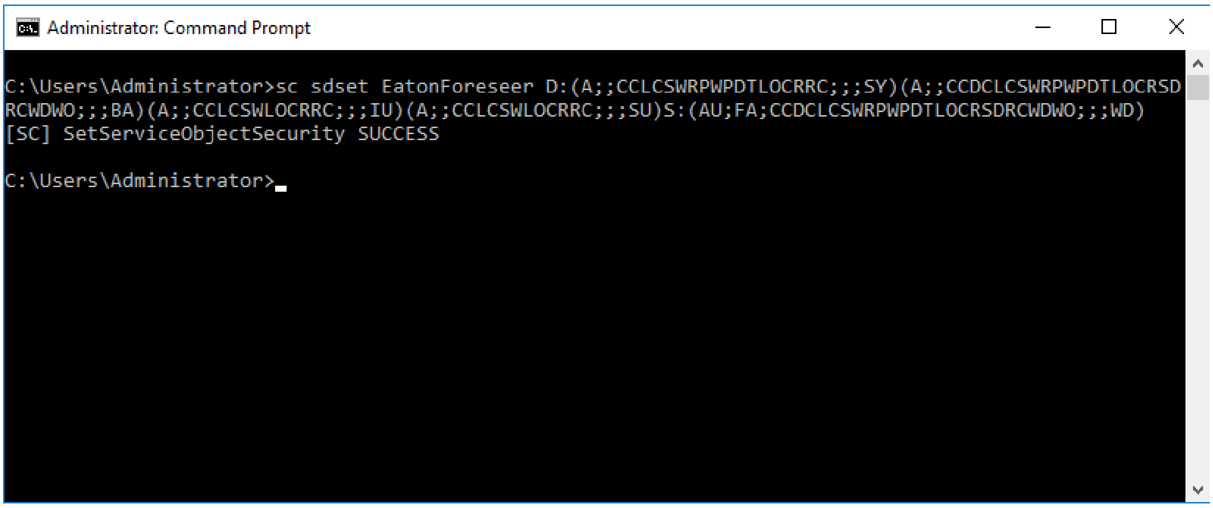
3. Privileges are assigned as a list of parenthetical citation. You will need to add a parenthetical citation to the list that includes the privilege string and SID of your designated user. You must add the citation prior to the "S:" designation. Assigning your user access by adding the following string with USERSID replaced with the actual account SID from Step 1 of this procedure.

(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;USERSID)



```
;U)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-687051253-3372532351-1810115475-1112)S:(AU;FA;CCDCI
```

4. Finally, copy the entire modified string. At a command prompt, run "sc sdset EatonForeseer <copied string from text editor>". Press Enter. You will receive a SUCCESS message once the process is complete.

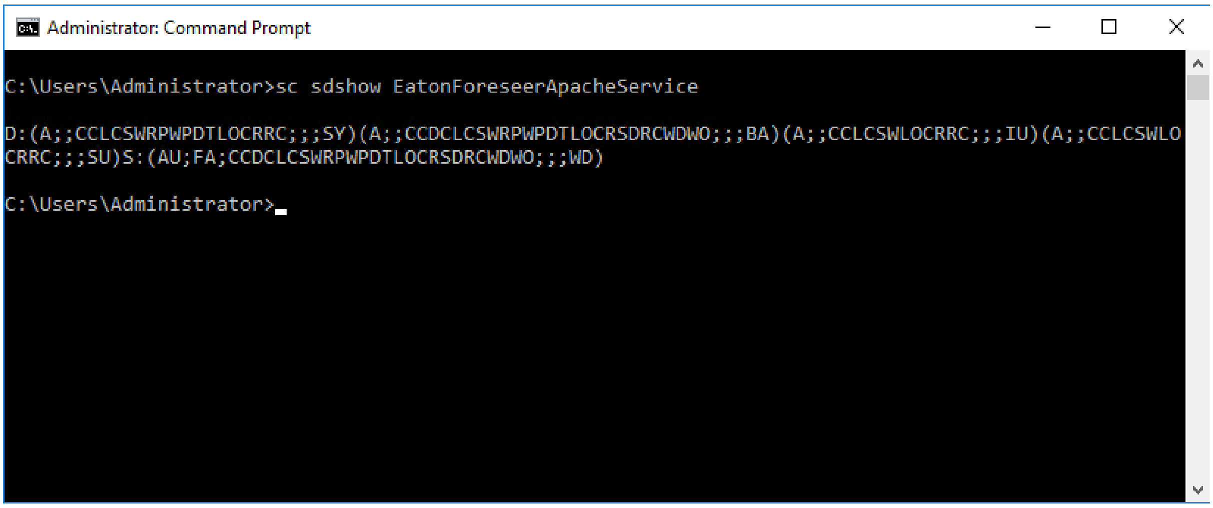


```
C:\Users\Administrator>sc sdset EatonForeseer D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
[SC] SetServiceObjectSecurity SUCCESS

C:\Users\Administrator>
```

Part 4 - Granting Access to Foreseer Apache

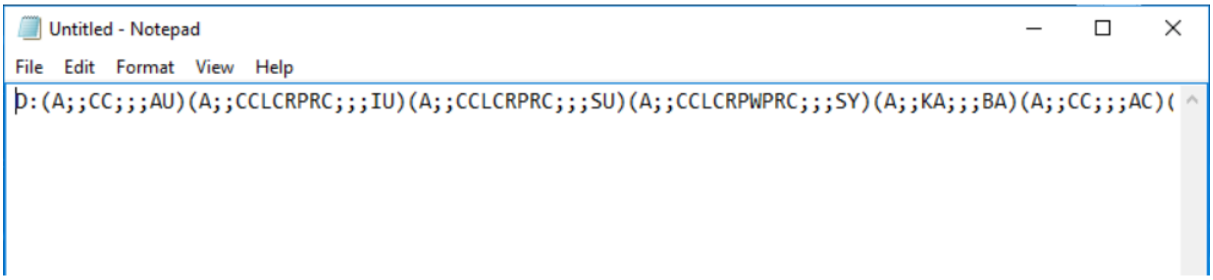
The Foreseer Apache service provides all web server functionality for the EPMS. It is started, stopped, and restarted anytime the Foreseer service is. To add your user account, perform the following steps:

1. From a command prompt, run "sc sdshow EatonForeseerApacheService". It will return something like this:



```
C:\Users\Administrator>sc sdshow EatonForeseerApacheService

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLO
CRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

C:\Users\Administrator>
```

2. Copy the entire string and paste into a text editor.

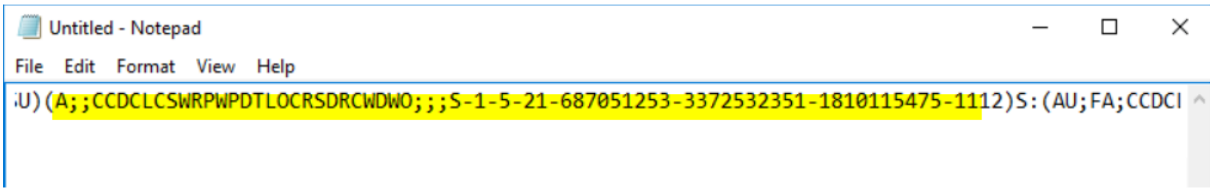


```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(
```

3. Privileges are assigned as a list of parenthetical citation. You will need to add a

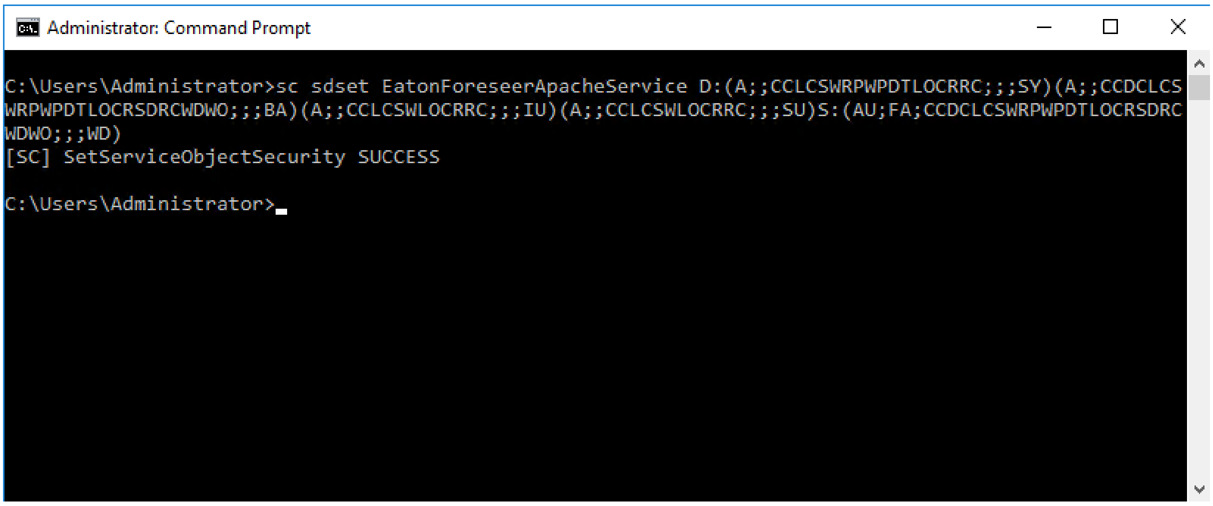
parenthetical citation to the list that includes the privilege string and SID of your designated user. You must add the citation prior to the “S:” designation. Assigning your user access by adding the following string with USERSID replaced with the actual account SID from Step 1 of this procedure.

(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;USERSID)



```
iU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-687051253-3372532351-1810115475-1112)S:(AU;FA;CCDCI
```

4. Finally, copy the entire modified string. At a command prompt, run “sc sdset EatonForeseerApacheService <copied string from text editor>”. Press Enter. You will receive a SUCCESS message once the process is complete.

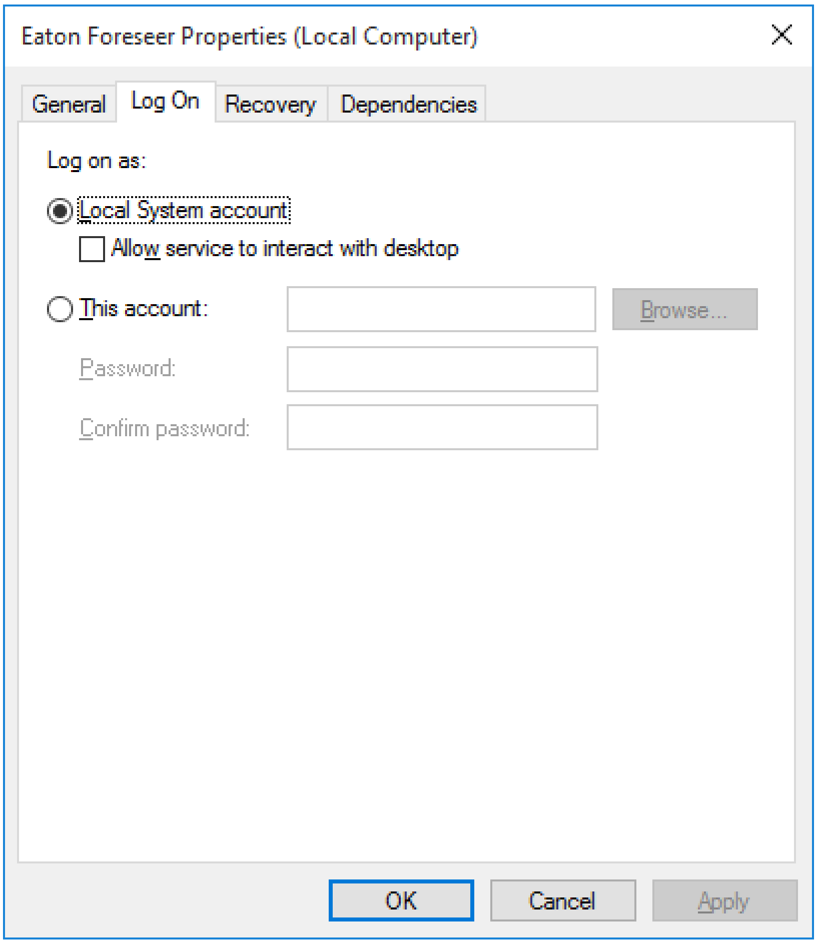


```
C:\Users\Administrator>sc sdset EatonForeseerApacheService D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)
[SC] SetServiceObjectSecurity SUCCESS

C:\Users\Administrator>_
```

Configure Foreseer and Apache Service Log On

Finally, you can now configure the Foreseer and Apache service log on for the specified user. Perform the following steps:

1. Access Control Panel>Administrative Tools>Services
2. Find the Eaton Foreseer service. Right-click and select Properties.
3. By default, the **Eaton Foreseer** service will utilize the Local System account. Click to select the *This account:* radio button. Then, browse and find the designated user that will run the service.



Eaton Foreseer Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

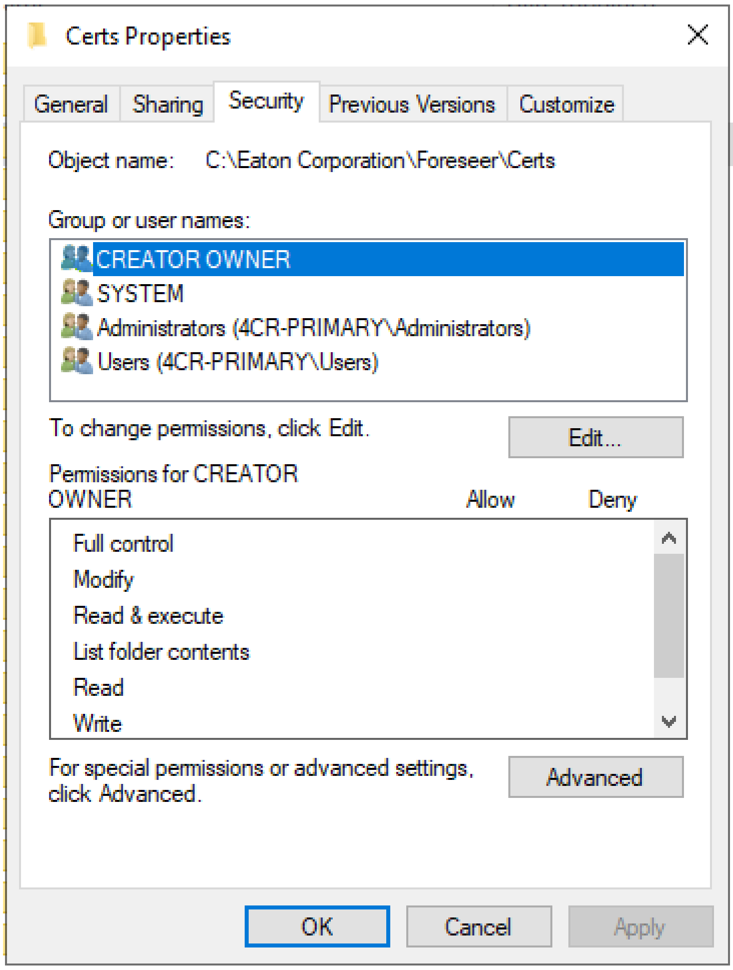
Confirm password:

4. Be sure to enter the password for the user account. Then click OK.   A restart of the service is necessary for this change to take effect.
5. Repeat Steps 3 through 5 for the **Eaton Foreseer Apache Service**.

Securing Web Certificates

Foreseer and it's Apache web-server will automatically start off using a self signed certificate and private key file. At any time, users can replace these self signed items with ones generated by a Certificate Authority or other provider of secure tokens.

All certificate and key are are commonly stored in the \Certs\ directory of your Foreseer installation. On a default installation in Windows, all users may have access to this folder. System administrators should strongly consider limiting access to this folder solely to privileged users and service accounts used by Foreseer to operate on a daily basis.



Object name: C:\Eaton Corporation\Foreseer\Certs

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (4CR-PRIMARY\Administrators)
- Users (4CR-PRIMARY\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER

- Full control
- Modify
- Read & execute
- List folder contents
- Read
- Write

For special permissions or advanced settings, click Advanced.

You can access file folder permissions by by right-clicking on the Certs folder and selecting Properties. Then, access the Security tab. Using the supplied editor features, you can add and delete the necessary users, groups, or service accounts from this folder.

All installations tend to be different. There is no specific guidance other than following your site's security policies and procedures.

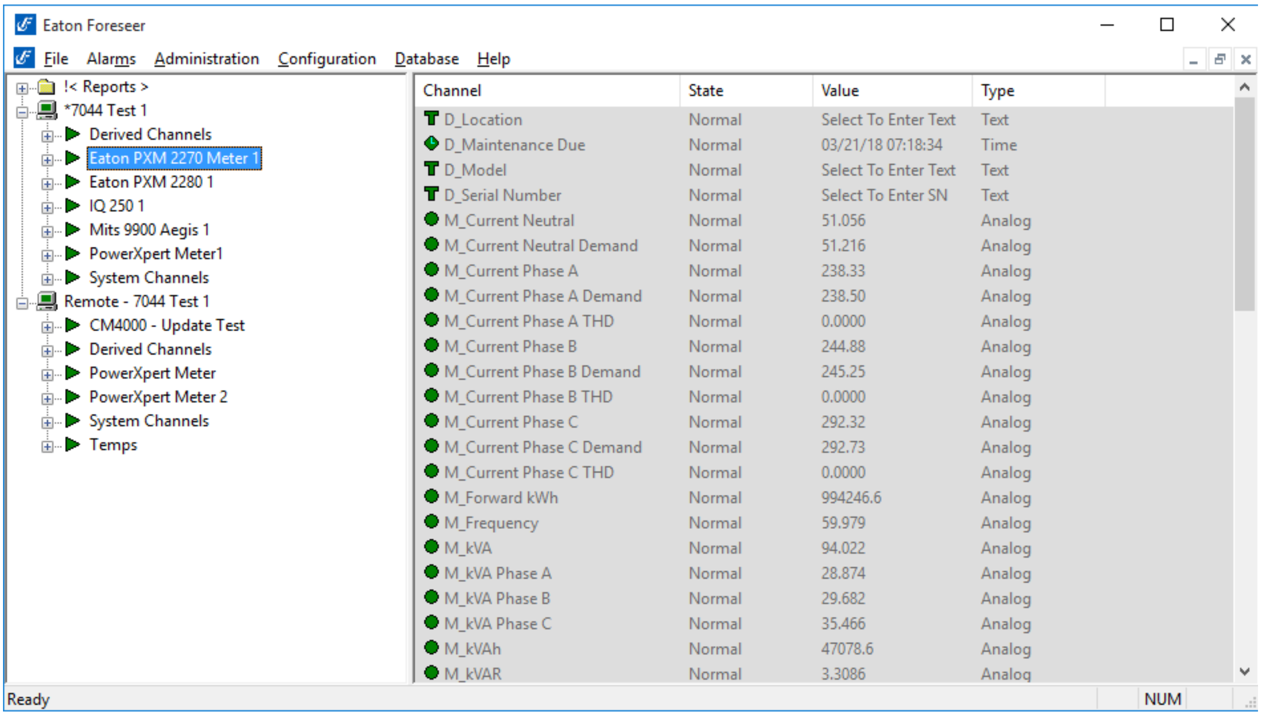
A full description of the processes and procedures for Access Control within the Windows operating system can be referenced at the following: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control

Foreseer Fundamentals

This section provides a high level overview of the Foreseer application. In most situations, setup and configuration changes are normally applied through Foreseer's WebConfiguration (WebConfig) utility, as well as the Device Configuration (DeviceConfig) utilities.

It may become necessary to run Foreseer as an application to change certain server configuration settings during installation, service, and even technical support.

The application window is comprised of several components which are consistently displayed throughout the program.



Channel	State	Value	Type
D_Location	Normal	Select To Enter Text	Text
D_Maintenance Due	Normal	03/21/18 07:18:34	Time
D_Model	Normal	Select To Enter Text	Text
D_Serial Number	Normal	Select To Enter SN	Text
M_Current Neutral	Normal	51.056	Analog
M_Current Neutral Demand	Normal	51.216	Analog
M_Current Phase A	Normal	238.33	Analog
M_Current Phase A Demand	Normal	238.50	Analog
M_Current Phase A THD	Normal	0.0000	Analog
M_Current Phase B	Normal	244.88	Analog
M_Current Phase B Demand	Normal	245.25	Analog
M_Current Phase B THD	Normal	0.0000	Analog
M_Current Phase C	Normal	292.32	Analog
M_Current Phase C Demand	Normal	292.73	Analog
M_Current Phase C THD	Normal	0.0000	Analog
M_Forward kWh	Normal	994246.6	Analog
M_Frequency	Normal	59.979	Analog
M_kVA	Normal	94.022	Analog
M_kVA Phase A	Normal	28.874	Analog
M_kVA Phase B	Normal	29.682	Analog
M_kVA Phase C	Normal	35.466	Analog
M_kVAh	Normal	47078.6	Analog
M_kVAR	Normal	3.3086	Analog

Foreseer employs dialog boxes to enter program information such as the properties which govern its various operations. Consistent with Windows displays, the information in some dialog boxes is grouped in categories under tabbed headings. Clicking on a tab selects that category and brings it to the front of the dialog box where the settings may be reviewed and altered. Scroll bars are automatically enabled whenever a dialog box selection list exceeds the available display area.

- Launching the Program
- Menu Bar
- Tree View
- Automatic Configuration Backups
- Exiting the Program

Launching the Program

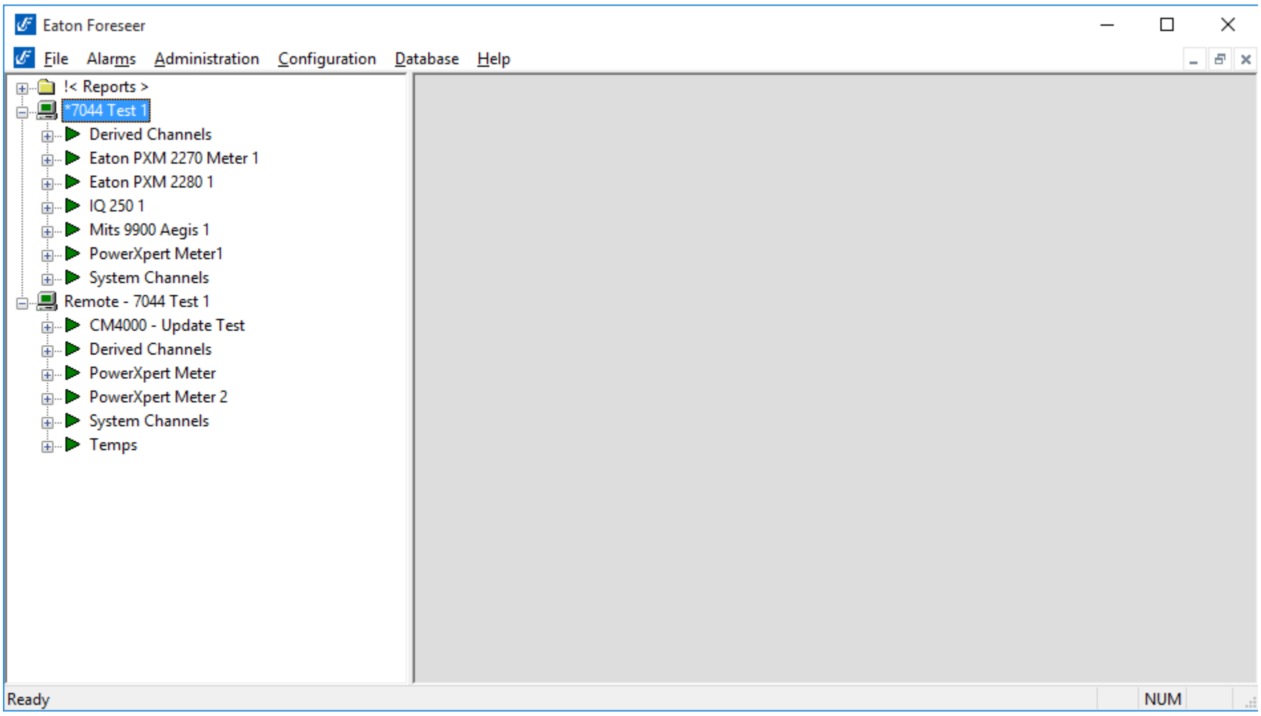
In order to launch Foreseer as an application, ensure that the Eaton Foreseer Server Service is not actively started. You can check the status of the service through Windows Administrative Tools. Administrative access is commonly required to start/stop/restart services.

To launch Foreseer as an application:

- Select Foreseer Server from the Window Start All Programs>Foreseer menu.

- Alternatively, you can launch Foreseer directly from its home installation path by double-clicking the Foreseer.exe program (commonly located in C:\Eaton Corporation\Foreseer).

Regardless of the method used to launch the Foreseer Server, the progress of its startup is displayed in a dialog box, followed by the program launching minimized to Windows Taskbar. To view the program, click to display it from the Taskbar.

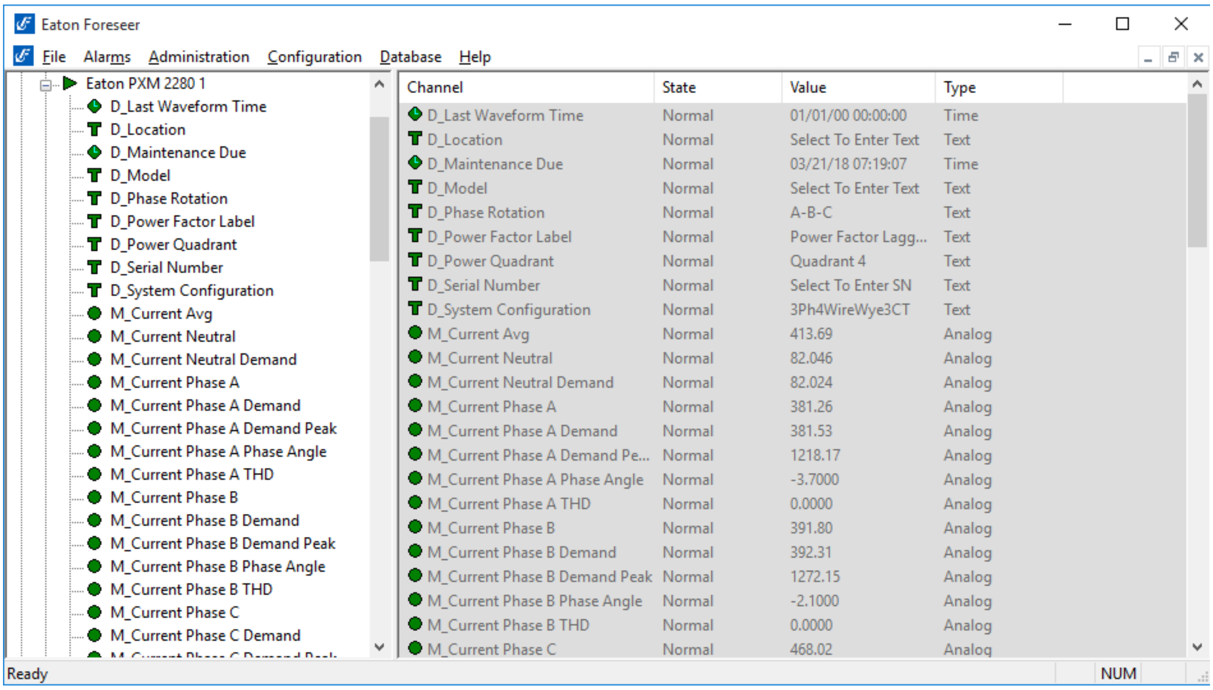


Menu Bar

The Menu Bar offers the standard Windows File and Help menus, as well as application-specific Alarms, Administration, Configuration, and Database, menus containing commands that are unique to Foreseer. Many of the commands are also available in the right-click, context-sensitive Tree View.

Tree View

The Tree View display scheme, previously called the Devices window, has expanded functionality.



- Eaton PXM 2280 1
  - D_Last Waveform Time
  - D_Location
  - D_Maintenance Due
  - D_Model
  - D_Phase Rotation
  - D_Power Factor Label
  - D_Power Quadrant
  - D_Serial Number
  - D_System Configuration
  - M_Current Avg
  - M_Current Neutral
  - M_Current Neutral Demand
  - M_Current Phase A
  - M_Current Phase A Demand
  - M_Current Phase A Demand Peak
  - M_Current Phase A Phase Angle
  - M_Current Phase A THD
  - M_Current Phase B
  - M_Current Phase B Demand
  - M_Current Phase B Demand Peak
  - M_Current Phase B Phase Angle
  - M_Current Phase B THD
  - M_Current Phase C
  - M_Current Phase C Demand

Channel	State	Value	Type
D_Last Waveform Time	Normal	01/01/00 00:00:00	Time
D_Location	Normal	Select To Enter Text	Text
D_Maintenance Due	Normal	03/21/18 07:19:07	Time
D_Model	Normal	Select To Enter Text	Text
D_Phase Rotation	Normal	A-B-C	Text
D_Power Factor Label	Normal	Power Factor Lagg...	Text
D_Power Quadrant	Normal	Quadrant 4	Text
D_Serial Number	Normal	Select To Enter SN	Text
D_System Configuration	Normal	3Ph4WireWye3CT	Text
M_Current Avg	Normal	413.69	Analog
M_Current Neutral	Normal	82.046	Analog
M_Current Neutral Demand	Normal	82.024	Analog
M_Current Phase A	Normal	381.26	Analog
M_Current Phase A Demand	Normal	381.53	Analog
M_Current Phase A Demand Pe...	Normal	1218.17	Analog
M_Current Phase A Phase Angle	Normal	-3.7000	Analog
M_Current Phase A THD	Normal	0.0000	Analog
M_Current Phase B	Normal	391.80	Analog
M_Current Phase B Demand	Normal	392.31	Analog
M_Current Phase B Demand Peak	Normal	1272.15	Analog
M_Current Phase B Phase Angle	Normal	-2.1000	Analog
M_Current Phase B THD	Normal	0.0000	Analog
M_Current Phase C	Normal	468.02	Analog

The left pane of the Tree View display lists all associated Foreseer Servers as well as their subordinate Devices and Channels. The list, like Windows Explorer, is expanded and contracted by clicking on the "**+**" and "**-**" preceding the desired icon. Selecting a Device displays summary information about its resident channels as well as the State, Value, and Type of each.

Selecting a Server, Device or Channel displays summary information about its constituent components in the right pane of the window. Listed Server information includes the Name, Address, frequency of Alarm and Channel Updates, whether the connection is Enabled, whether the configuration needs updating and when the Last Update Check was performed. Device information lists its resident channels as well as the State, Value and Type of each.

The use of leading characters (such as “*”, " ", and “!”) in list names are used to ensure critical elements sort at the top of the list in larger Server configurations. These can be server names or remote names or redundant names but cannot be included in device/channel names.

The Tree View also allows Reports to be created and viewed if needed.

Tree View Menu Commands

Selecting a Server, Device or Channel and right-clicking presents a context-sensitive menu that allows certain Foreseer actions and responses to be performed depending on the highlighted system component. Multiple items of the same type (Devices, for instance) can be selected for manipulation or modification as a group; channels of the same type

(Meters or Status) may be selected from different Devices for functions such as graphing.

> ✓ Any grayed commands are unavailable for the selected Server, Device or Channel: Some require Administrative Authorization to execute.

Alarms

Alarm Acknowledge - allows an alarm condition to be acknowledged on the selected channel(s). Once acknowledged, a channel's representative icons turns **blue**. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu if necessary.

Alarm Rearm - allows alarm monitoring to resume on the chosen channel(s). A System Generated Note that includes the time of the rearming and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu if necessary This command is only available for channels with an acknowledged alarm.

Alarm Ack/Rearm - permits an alarm condition to be acknowledged and the selected channel(s) to be rearmed so testing of acquired Values against set Alarm Limits resumes immediately. Acknowledged, a channel's icon turns **blue**. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu if necessary.

Disarm - suspends Alarm Limit testing for the selected Device(s) or channel(s). Channel data, however, continues to be archived. Disarming a channel is useful when making repairs to avoid reporting nuisance alarms.

Rearm - resumes Alarm Limit testing for the selected Device(s) or channel(s).

Install Device... - allows you to Install Devices on the Foreseer Server so that they may be monitored and added to the Client **WebViews**.

Add User-Defined Channel... - permits the User to create new Derived Channels.

Add Channel... - permits the User to create a new Meters (Analog) or Status (Digital) Channel. This command is not available for all Devices.

Disable - suspends data archiving for the selected Device(s) or channel(s). Disabling is useful when making repairs to avoid archiving inappropriate readings and is necessary in order to Delete or Rename a Device or channel.

Enable - resumes data archiving for the selected Device(s) or channel(s).

Delete - permanently deletes the selected Server, Device or Channel from the Server database. Once removed, its archived information is no longer available. Deleting a Device or Channel should be done with discretion as removing it can have an adverse affect on Foreseer WebViews configurations.

Rename - permits the selected Device or Channel to be renamed in response to changing conditions. It should be noted that renaming a Device or Channel should be done with discretion as changing a name can have an adverse effect on Foreseer WebViews configurations.

Copy Channel Properties - copies all of the currently selected channel's **Properties** to the Windows clipboard, allowing its settings to be pasted directly into another channel as its operational parameters. This command is useful when applied to an entire Device (rather than individual channels) for quickly setting up multiple Devices that contain similar channels. In either case, the channel or Device being copied **must be of the exact same type** as the one the **Properties** are being pasted into.

Paste Channel Properties - pastes the previously copied **Properties** into the currently selected channel as its operational parameters. It also is useful when duplicating numerous channel settings on multiple Devices. In either case, the channel or Device being pasted into **must be of the exact same type** as the one the **Properties** are being copied from. these settings then can be individually modified as necessary. If copying from a Device (rather than a single channel), only those channels with the same Name will have their **Properties** pasted.

Properties... - displays the Device Properties, Meters (Analog), or Status (Digital) **Channel Properties**, depending upon which is selected.

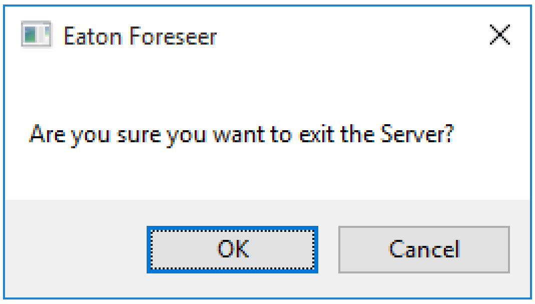
Exiting the Program

Exiting terminates the current Foreseer Server session. There are several ways to quit the program:

- Select the Close command under the Foreseer icon in the application's title bar.
- Click on the Windows Close button in the application's title bar.
- Select the Exit command in the Foreseer menu.
- Simultaneously press the **Alt** and **F4** keys.

Regardless of the method you choose to quit the Foreseer application, you are prompted to confirm that you wish to terminate the session. Press OK to end the current session; Cancel returns to program operation.

✓ Administrative Authorization is required to Exit the application.



Are you sure you want to exit the Server?

Menu Reference

This section describes the menu items available in the Foreseer application. Those menu items are:

- File Menu
- Alarms Menu
- Administration Menu
- Configuration Menu
- Database Menu
- Help Menu

File Menu

The **File** menu furnishes one basic program command: the ability to quit the program:

✓ Administrative Authorization may be required to execute this command.

Exit - terminates the current Foreseer Server session. If enabled during initial Server configuration, you are required to have Administrative Authorization to quit the program.

Alarms Menu

The **Alarms** menu allows you to respond to reported alarm conditions in several ways. This menu also is accessed by right-clicking with the mouse pointer positioned in the **Tree View**. Any grayed commands are not available for the currently chosen Server, Device or Channel. Multiple Devices or Channels of the same type may be chosen for modification using the standard Windows Shift-Click and Ctrl-Click selection methods.

✓ Administrative Authorization is required before you can perform Alarm Management functions.

The **Alarms** menu offers the following Foreseer commands:

Alarm Acknowledge - Allows an alarm condition to be acknowledged on the selected channel(s). Once acknowledged, a channel's representative icons turns **blue**. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu if necessary.

Alarm Rearm - Allows alarm monitoring to resume on the chosen channel(s). A System Generated Note that includes the time of the rearming and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu. This command is only available for channels with an acknowledged alarm.

Alarm Ack/Rearm - Permits an alarm condition to be acknowledged and the selected channel(s) to be rearmed so testing of acquired Values against set Alarm Limits resumes immediately. Acknowledged, a channel's icon turns **blue**. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional **Notes** may be entered through the Add Note... command in the Administration menu.

- Alarms Acknowledge
- Alarm Rearm
- Acknowledging and Rearming Alarms

Alarm Latching is a toggle state which determines whether an alarm condition continues to be reported if the channel's Current Value returns to within its assigned Critical or Cautionary Alarm Limits. When Enabled the channel's highest alarm state is reported regardless of its Current Value, a channel is automatically removed from theStatus Bar's Active Alarm Totals if its Value returns to within its specified Limits. Note that the alarms must be Enabled and Limits assigned under the **Basic** tab in the channel's Meters or Status **Channel Properties** dialog box. The Re-Arm period (one hour by default) is specified under the **Advanced** tab in the channel's Meters or Status **Channel Properties** dialog box.

Hysteresis, when Enabled, determines the threshold Value before a new alarm is reported for a Meters channel. Hysteresis is used to eliminate nuisance alarms when the channel's input is near its Alarm Limit. Once an alarm occurs, the input level must drop below or rise above the threshold Value then exceed the Limit once again before a new alarm is reported. The particular threshold Value is specified in the channel's display Units (i.e., volts, amps, hz, kVA, kw, etc.). Note that this attribute is only available for non-Latching alarms.

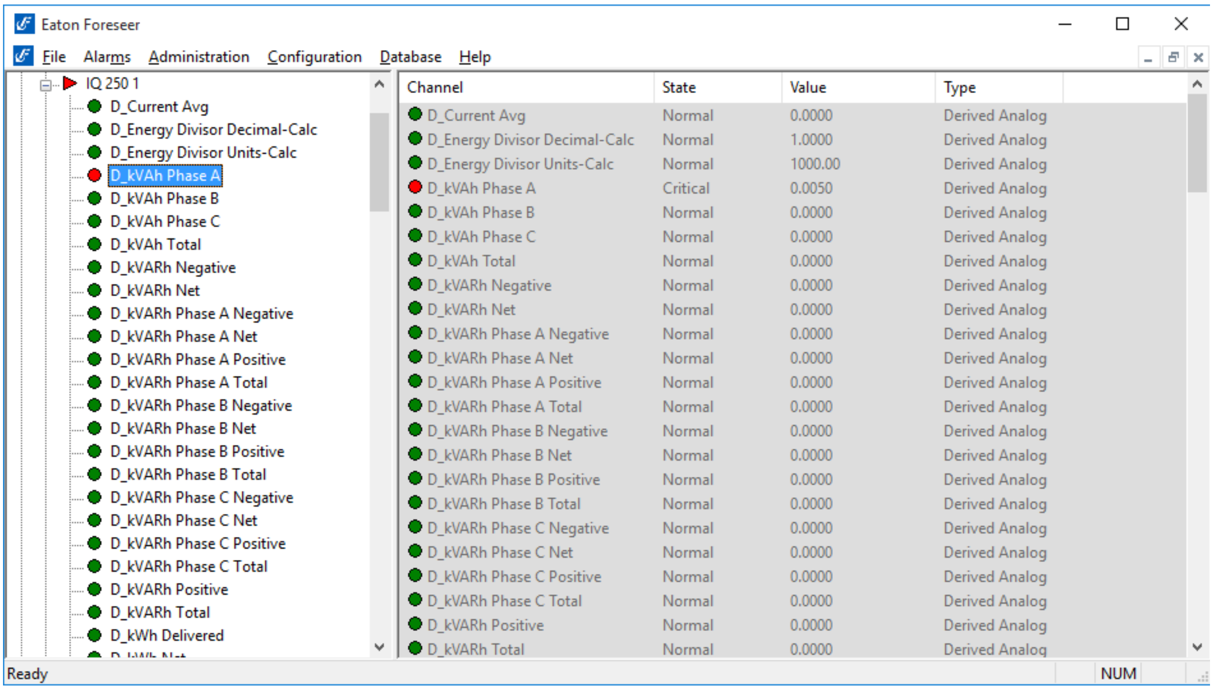
Alarm Acknowledge

The Foreseer Server allows for limited Alarm Management responses. Channel alarm conditions can be Acknowledged and Rearmed through the Alarms menu and the Tree View. A **Note** may be required to further document the situation.

To access the Foreseer Server Alarm Management capabilities:

> ✓ Administrative Authorization may be required to Acknowledge and/or Rearm alarms.

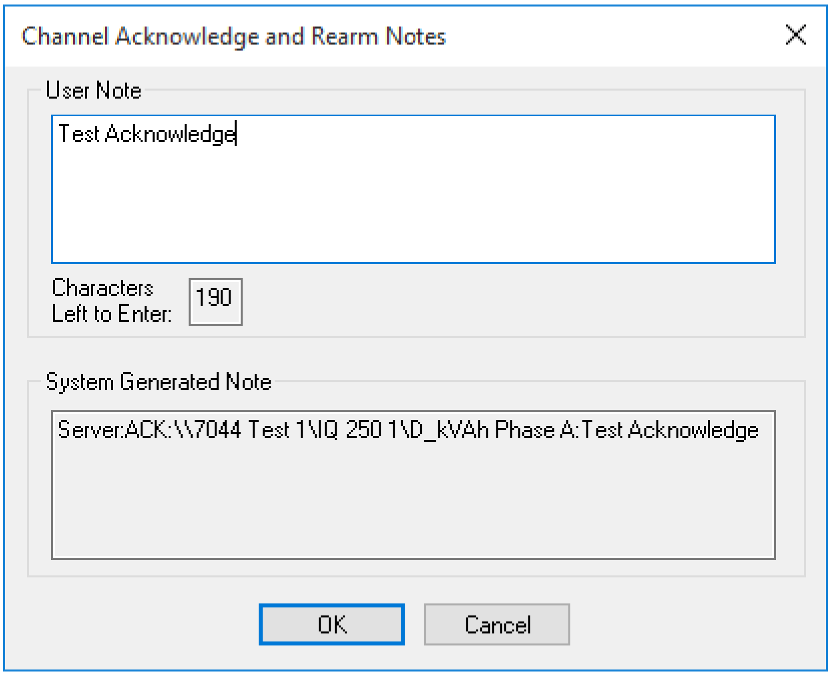
1. The desired alarm channel(s) can be highlighted in the left pane of the **Tree View**. Multiple channels may be selected by holding down the **Ctrl** key and clicking on them individually. Holding down the **Shift** key while clicking on two channels selects all channels between them.
2. WIth the desired channel(s) selected, right-click and choose the desired Alarm command--Acknowledge, Rearm or Ack/Rearm.



IQ 250 1
- D_Current Avg
- D_Energy Divisor Decimal-Calc
- D_Energy Divisor Units-Calc
- D_kVAh Phase A
- D_kVAh Phase B
- D_kVAh Phase C
- D_kVAh Total
- D_kVARh Negative
- D_kVARh Net
- D_kVARh Phase A Negative
- D_kVARh Phase A Net
- D_kVARh Phase A Positive
- D_kVARh Phase A Total
- D_kVARh Phase B Negative
- D_kVARh Phase B Net
- D_kVARh Phase B Positive
- D_kVARh Phase B Total
- D_kVARh Phase C Negative
- D_kVARh Phase C Net
- D_kVARh Phase C Positive
- D_kVARh Phase C Total
- D_kVARh Positive
- D_kVARh Total
- D_kWh Delivered
- D_kWh Net

Channel	State	Value	Type
D_Current Avg	Normal	0.0000	Derived Analog
D_Energy Divisor Decimal-Calc	Normal	1.0000	Derived Analog
D_Energy Divisor Units-Calc	Normal	1000.00	Derived Analog
D_kVAh Phase A	Critical	0.0050	Derived Analog
D_kVAh Phase B	Normal	0.0000	Derived Analog
D_kVAh Phase C	Normal	0.0000	Derived Analog
D_kVAh Total	Normal	0.0000	Derived Analog
D_kVARh Negative	Normal	0.0000	Derived Analog
D_kVARh Net	Normal	0.0000	Derived Analog
D_kVARh Phase A Negative	Normal	0.0000	Derived Analog
D_kVARh Phase A Net	Normal	0.0000	Derived Analog
D_kVARh Phase A Positive	Normal	0.0000	Derived Analog
D_kVARh Phase A Total	Normal	0.0000	Derived Analog
D_kVARh Phase B Negative	Normal	0.0000	Derived Analog
D_kVARh Phase B Net	Normal	0.0000	Derived Analog
D_kVARh Phase B Positive	Normal	0.0000	Derived Analog
D_kVARh Phase B Total	Normal	0.0000	Derived Analog
D_kVARh Phase C Negative	Normal	0.0000	Derived Analog
D_kVARh Phase C Net	Normal	0.0000	Derived Analog
D_kVARh Phase C Positive	Normal	0.0000	Derived Analog
D_kVARh Phase C Total	Normal	0.0000	Derived Analog
D_kVARh Positive	Normal	0.0000	Derived Analog
D_kVARh Total	Normal	0.0000	Derived Analog

3. Enter the User Notes for this alarm



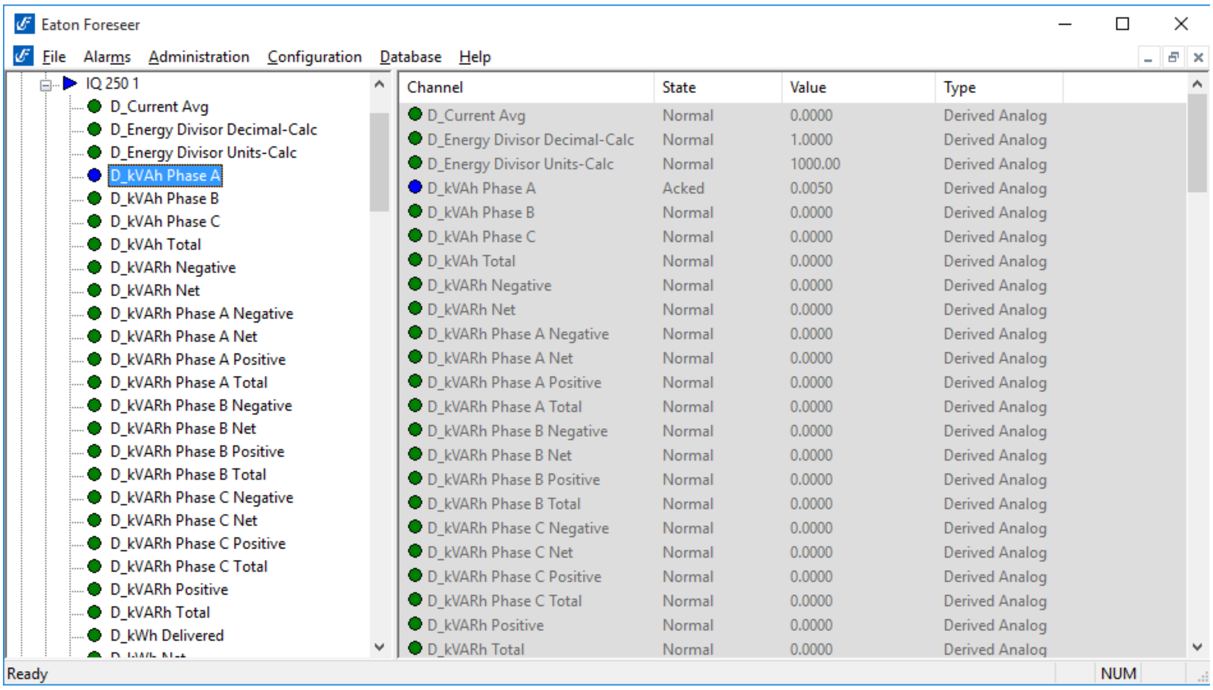
Channel Acknowledge and Rearm Notes
User Note
Characters Left to Enter:
System Generated Note
OK
Cancel

User Note: Test Acknowledge

Characters Left to Enter: 190

System Generated Note: Server:ACK:\\7044 Test 1\IQ 250 1\D_kVAh Phase A:Test Acknowledge

4. Click OK to exit this dialog



Channel	State	Value	Type
● D_Current Avg	Normal	0.0000	Derived Analog
● D_Energy Divisor Decimal-Calc	Normal	1.0000	Derived Analog
● D_Energy Divisor Units-Calc	Normal	1000.00	Derived Analog
● D_kVAh Phase A	Acked	0.0050	Derived Analog
● D_kVAh Phase B	Normal	0.0000	Derived Analog
● D_kVAh Phase C	Normal	0.0000	Derived Analog
● D_kVAh Total	Normal	0.0000	Derived Analog
● D_kVARh Negative	Normal	0.0000	Derived Analog
● D_kVARh Net	Normal	0.0000	Derived Analog
● D_kVARh Phase A Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase A Net	Normal	0.0000	Derived Analog
● D_kVARh Phase A Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase A Total	Normal	0.0000	Derived Analog
● D_kVARh Phase B Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase B Net	Normal	0.0000	Derived Analog
● D_kVARh Phase B Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase B Total	Normal	0.0000	Derived Analog
● D_kVARh Phase C Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase C Net	Normal	0.0000	Derived Analog
● D_kVARh Phase C Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase C Total	Normal	0.0000	Derived Analog
● D_kVARh Positive	Normal	0.0000	Derived Analog
● D_kVARh Total	Normal	0.0000	Derived Analog

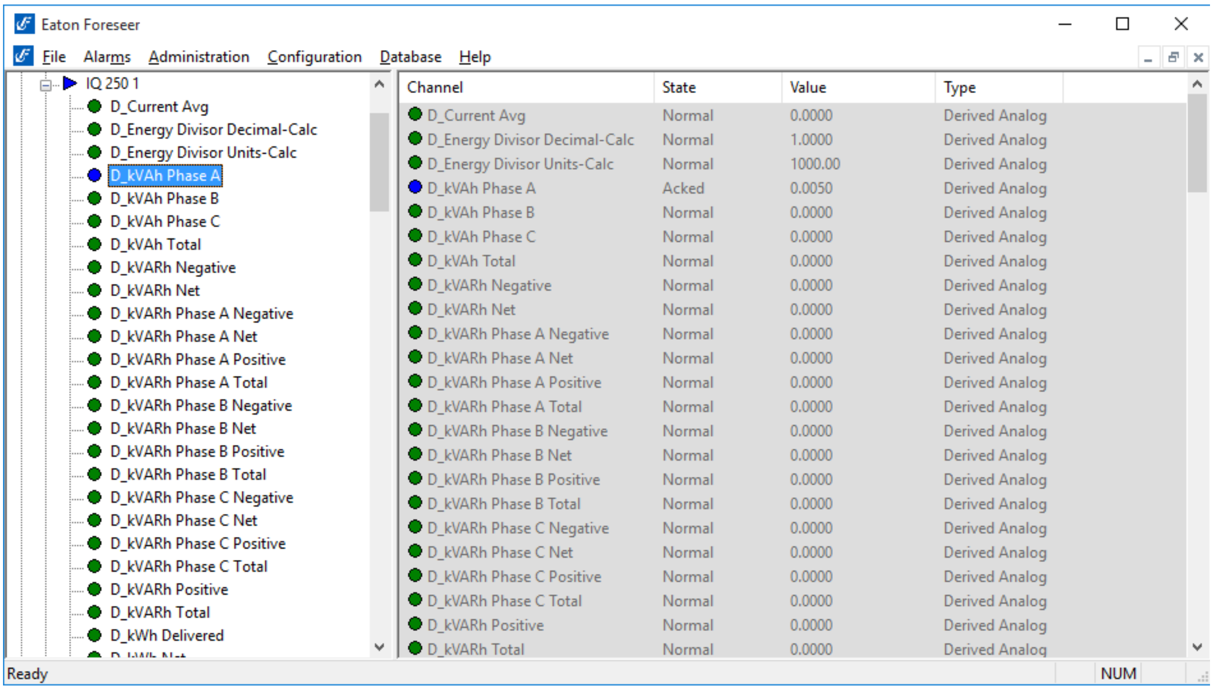
Alarm Rearm

The Foreseer Server allows for limited Alarm Management responses. Channel alarm conditions can be Acknowledged and Rearmed through the Alarms menu and the Tree View. A **Note** may be required to further document the situation.

To access the Foreseer Server Alarm Management capabilities:

Administrative Authorization may be required to Acknowledge and/or Rearm alarms.

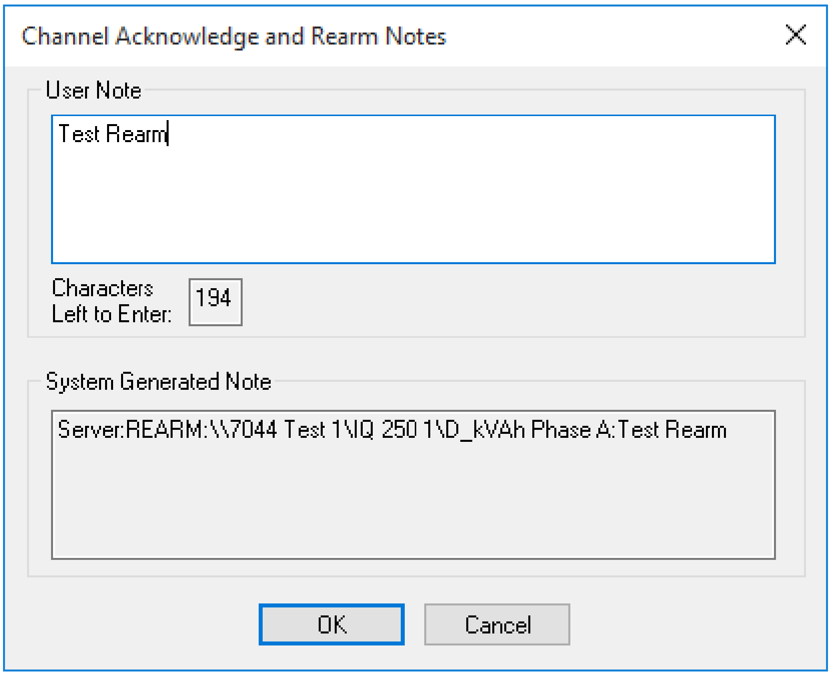
1. The desired alarm channel(s) can be highlighted in the left pane of the **Tree View**. Multiple channels may be selected by holding down the **Ctrl** key and clicking on them individually. Holding down the **Shift** key while clicking on two channels selects all channels between them.



- IQ 250 1
  - D_Current Avg
  - D_Energy Divisor Decimal-Calc
  - D_Energy Divisor Units-Calc
  - D_kVAh Phase A
  - D_kVAh Phase B
  - D_kVAh Phase C
  - D_kVAh Total
  - D_kVARh Negative
  - D_kVARh Net
  - D_kVARh Phase A Negative
  - D_kVARh Phase A Net
  - D_kVARh Phase A Positive
  - D_kVARh Phase A Total
  - D_kVARh Phase B Negative
  - D_kVARh Phase B Net
  - D_kVARh Phase B Positive
  - D_kVARh Phase B Total
  - D_kVARh Phase C Negative
  - D_kVARh Phase C Net
  - D_kVARh Phase C Positive
  - D_kVARh Phase C Total
  - D_kVARh Positive
  - D_kVARh Total
  - D_kWh Delivered

Channel	State	Value	Type
D_Current Avg	Normal	0.0000	Derived Analog
D_Energy Divisor Decimal-Calc	Normal	1.0000	Derived Analog
D_Energy Divisor Units-Calc	Normal	1000.00	Derived Analog
D_kVAh Phase A	Acked	0.0050	Derived Analog
D_kVAh Phase B	Normal	0.0000	Derived Analog
D_kVAh Phase C	Normal	0.0000	Derived Analog
D_kVAh Total	Normal	0.0000	Derived Analog
D_kVARh Negative	Normal	0.0000	Derived Analog
D_kVARh Net	Normal	0.0000	Derived Analog
D_kVARh Phase A Negative	Normal	0.0000	Derived Analog
D_kVARh Phase A Net	Normal	0.0000	Derived Analog
D_kVARh Phase A Positive	Normal	0.0000	Derived Analog
D_kVARh Phase A Total	Normal	0.0000	Derived Analog
D_kVARh Phase B Negative	Normal	0.0000	Derived Analog
D_kVARh Phase B Net	Normal	0.0000	Derived Analog
D_kVARh Phase B Positive	Normal	0.0000	Derived Analog
D_kVARh Phase B Total	Normal	0.0000	Derived Analog
D_kVARh Phase C Negative	Normal	0.0000	Derived Analog
D_kVARh Phase C Net	Normal	0.0000	Derived Analog
D_kVARh Phase C Positive	Normal	0.0000	Derived Analog
D_kVARh Phase C Total	Normal	0.0000	Derived Analog
D_kVARh Positive	Normal	0.0000	Derived Analog
D_kVARh Total	Normal	0.0000	Derived Analog

2. Enter the User Notes for this alarm



Channel Acknowledge and Rearm Notes

User Note

Test Rearm

Characters Left to Enter: 194

System Generated Note

Server:REARM:\\7044 Test 1\IQ 250 1\D_kVAh Phase A:Test Rearm

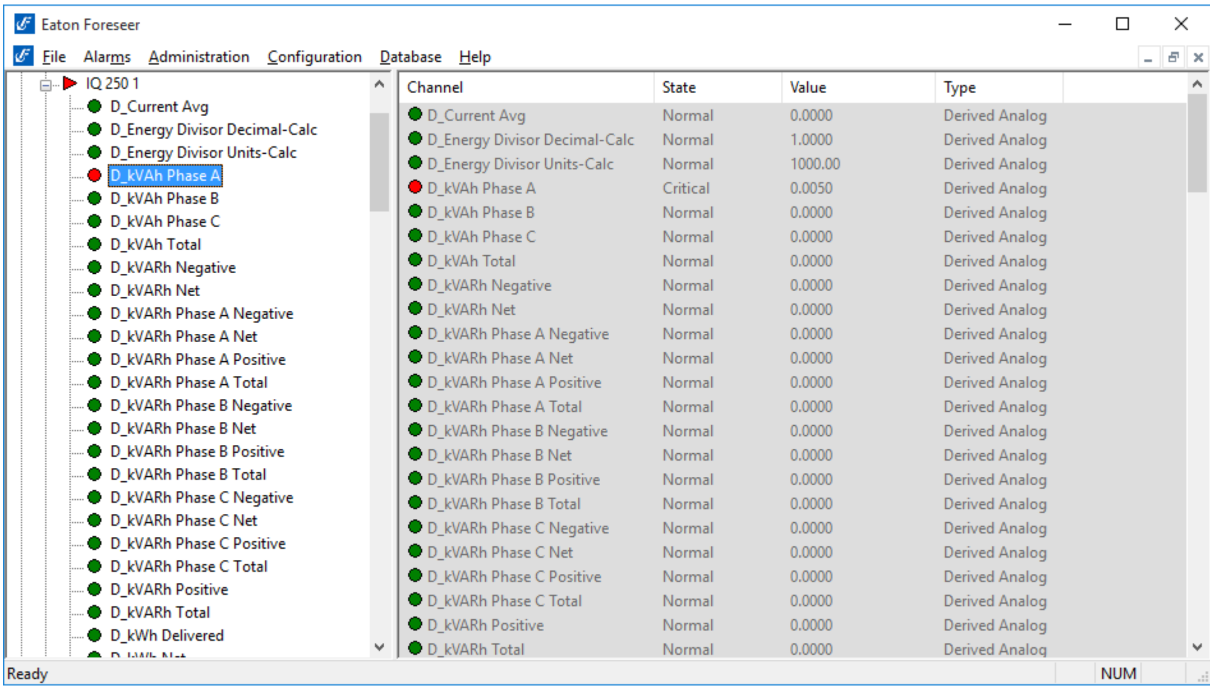
Acknowledging and Rearming Alarms

Acknowledgment suspends limit testing on the alarm channel in order to allow the problem to be serviced although the channel's Value continues to be calculated and archived. The context-sensitive Tree View menu allows limited alarm response at the Server. More comprehensive responses to alarm conditions are available through the Foreseer WebViews client.

> ✓ Administrative Authorization may be required to Acknowledge and/or Rearm alarms.

To acknowledge a channel alarm:

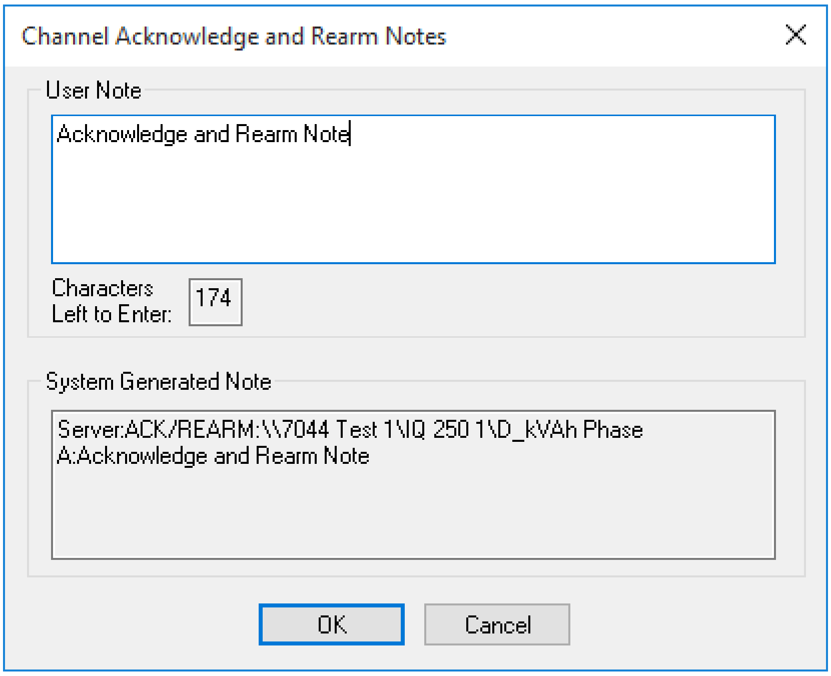
1. Click on the affected channel to highlight it. Multiple channels may be selected by holding down the **Ctrl** key and clicking on them individually. Holding down the **Shift** key while clicking on two channels selects all channels between them.
2. Choose Alarm Acknowledge from the Alarms menu. You can also choose Alarm Ack/Rearm to immediately Rearm the channel and resume testing of its acquired Value against its set Alarm Limits.



Channel	State	Value	Type
● D_Current Avg	Normal	0.0000	Derived Analog
● D_Energy Divisor Decimal-Calc	Normal	1.0000	Derived Analog
● D_Energy Divisor Units-Calc	Normal	1000.00	Derived Analog
● D_kVAh Phase A	Critical	0.0050	Derived Analog
● D_kVAh Phase B	Normal	0.0000	Derived Analog
● D_kVAh Phase C	Normal	0.0000	Derived Analog
● D_kVAh Total	Normal	0.0000	Derived Analog
● D_kVARh Negative	Normal	0.0000	Derived Analog
● D_kVARh Net	Normal	0.0000	Derived Analog
● D_kVARh Phase A Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase A Net	Normal	0.0000	Derived Analog
● D_kVARh Phase A Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase A Total	Normal	0.0000	Derived Analog
● D_kVARh Phase B Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase B Net	Normal	0.0000	Derived Analog
● D_kVARh Phase B Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase B Total	Normal	0.0000	Derived Analog
● D_kVARh Phase C Negative	Normal	0.0000	Derived Analog
● D_kVARh Phase C Net	Normal	0.0000	Derived Analog
● D_kVARh Phase C Positive	Normal	0.0000	Derived Analog
● D_kVARh Phase C Total	Normal	0.0000	Derived Analog
● D_kVARh Positive	Normal	0.0000	Derived Analog
● D_kVARh Total	Normal	0.0000	Derived Analog

3. If a Password was specified, you are prompted to enter the Administrative Authorization before proceeding. Another authorized user can temporarily log on to acknowledge an alarm without affecting the current user's session. This allows the response to be recorded under that person's name, or he has the option of becoming the currently logged in user.
4. You are also prompted to enter a Foreseer **Note** in the **Channel Acknowledgment**

and Rearm Notes dialog box to document additional information or observations about the alarm condition(s). The **Note** is limited to 256 characters and includes the time and date it was entered, as well as other relevant information. Once Acknowledged, the channel's icon turns **blue** to indicate its state. Additional **Notes** may be entered through the Add Note... command in the Administration menu if necessary.


Channel Acknowledge and Rearm Notes
User Note

Acknowledge and Rearm Note

Characters Left to Enter:

174

Server:ACK/REARM:\\7044 Test 1\IQ 250 1\D_kVAh Phase A:Acknowledge and Rearm Note

Administration Menu

The **Administration** menu contains various system functions. Many **Administration** commands display a dialog box which requires additional input before the particular operation can be performed. Any grayed commands cannot be performed on the selected item or within the active window.

✓ Administrative Authorization is required before proceeding with any of these commands.

The **Administration** menu offers the following Foreseer commands:

Login... - records the beginning of the current User's session.

Logoff... - records the end of the current User's session.

Change Password... - allows the current Administrative and Change Database Password to be altered.

Add Note... - opens the Add a Note dialog box, allowing user observations to be entered into the database.

Message Management > - allows you to Setup the **Message Management** feature and Configure Required Connections. It also accesses the (optional) *SNMP Properties*. For more details on configuring Message Management, please consult the Message Manager Guide for additional details.

WebViews Server > - allows an HTTP (non-secure) or an HTTPS (secure) WebViews Server to be created and viewed through a Microsoft Internet Explorer.

Trusted Web Clients... - is a list of IP addresses or machine names defining the set of web clients allowed to access WebViews / WebAdmin.

Extension Plugins... - is reserved for future program enhancements.

Unload Driver - is a File Management function which clears the driver file for the selected Device. Multiple Devices of the same Type may be selected for unloading without shutting the system down. This function should only be performed at the direction of Eaton technical support.

Load Driver - is a File Management function which automatically loads the appropriate Device driver from the Update VI folder. Multiple Devices of the same Type may be selected for loading without shutting the system down. This function should only be performed at the direction of Eaton technical support.

Server Properties... - displays the Server Properties dialog box, allowing certain program parameters to be altered.

Server Properties

The Server Properties dialog box, accessed through the Server Properties command in the Administration menu, allows several general settings to be specified. They are organized under four tabs:

General provides the name of the Foreseer Server whenever it is reported, such as in Message Management and in Report titles. It also quantifies the information that is written to the Log file. Other settings permit the Server to be enabled as a password- protected user rather than a local system account when running as a service, enabling a delay in startup, and Watchdog Processing support to ensure ongoing system operation.

Remote settings allow WebViews Administrative users to restart the Foreseer application on the Server, perform a complete reboot of the Foreseer Server computer, and upload newer releases of Foreseer software and Device Drivers to the Foreseer Server.

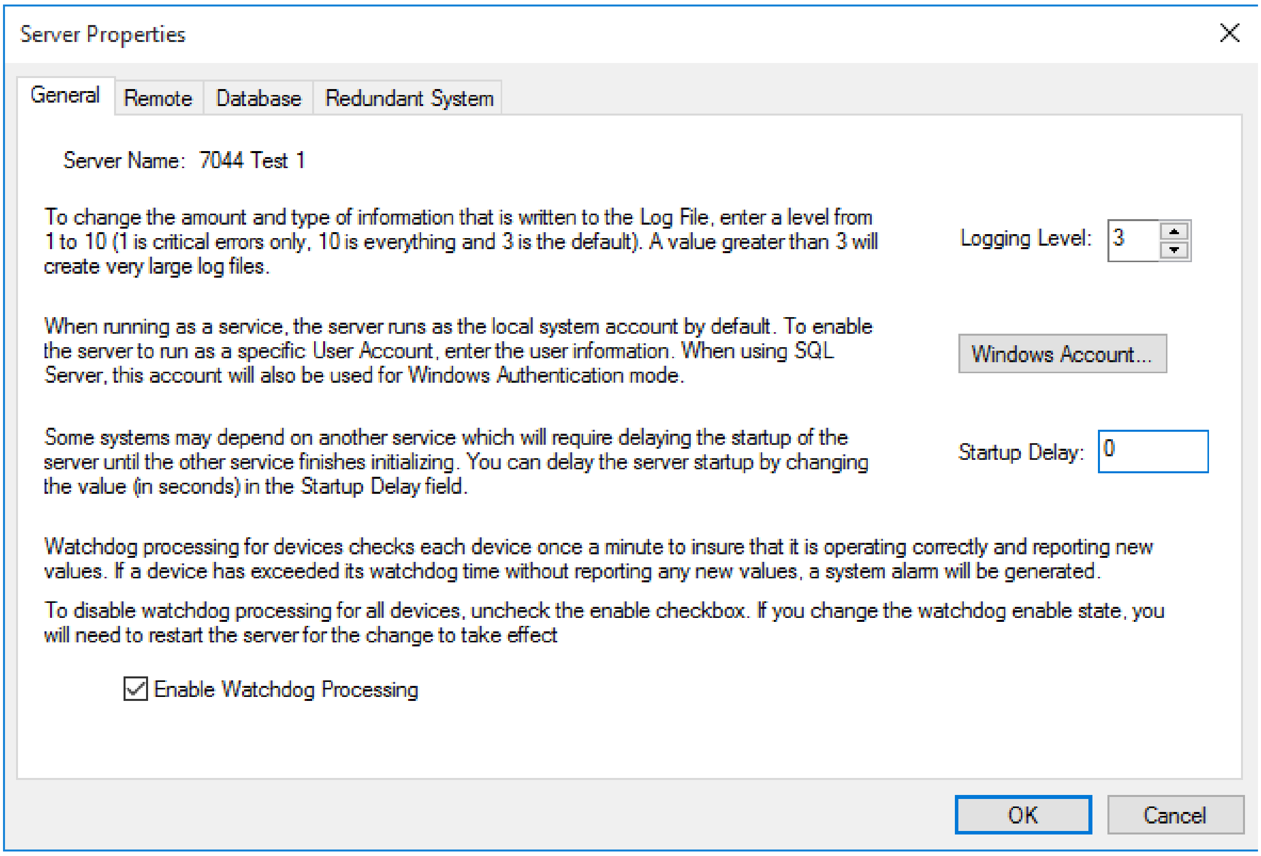
Database specifies a Retry Time, in seconds, after which Foreseer will attempt to reconnect to SQL Server. Foreseer will continue to retry connections, using the specified interval between tries, until a connection is established. The retry attempts can be temporarily disabled to avoid nuisance alarms, or this feature can be disabled entirely through the check box.

Redundant System identifies the Server as a backup to ensure continued site monitoring in the event the principal Server fails. A single redundant Server is designated as a Stand-Alone. In instances where there is more than one such Server, it must be identified as the Primary or Secondary Redundant in the backup system.

- Server Properties - General
- Server Properties - Remote
- Server Properties - Database
- Server Properties - Redundant System

Server Properties - General

The Server Properties dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **General Properties** identifies the Server and configures startup. Click on other tabs to present those **Server Properties**.



Server Name: 7044 Test 1

To change the amount and type of information that is written to the Log File, enter a level from 1 to 10 (1 is critical errors only, 10 is everything and 3 is the default). A value greater than 3 will create very large log files.

Logging Level: 3

When running as a service, the server runs as the local system account by default. To enable the server to run as a specific User Account, enter the user information. When using SQL Server, this account will also be used for Windows Authentication mode.

Some systems may depend on another service which will require delaying the startup of the server until the other service finishes initializing. You can delay the server startup by changing the value (in seconds) in the Startup Delay field.

Startup Delay: 0

Watchdog processing for devices checks each device once a minute to insure that it is operating correctly and reporting new values. If a device has exceeded its watchdog time without reporting any new values, a system alarm will be generated.

To disable watchdog processing for all devices, uncheck the enable checkbox. If you change the watchdog enable state, you will need to restart the server for the change to take effect

☑ Enable Watchdog Processing

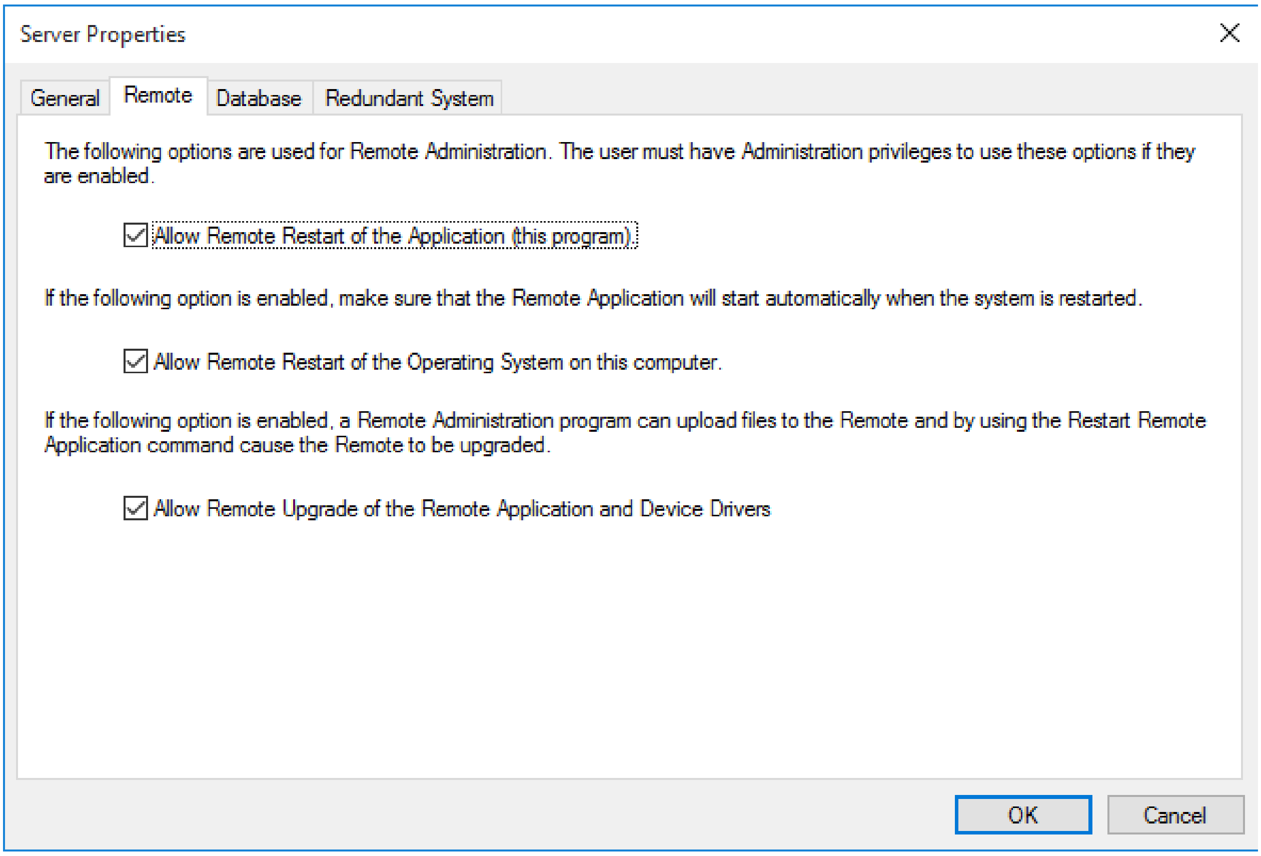
To specify General Server Properties:

✓ Administrative Authorization is required to access **Server Properties**.

1. Select Server Properties... in the Administration menu.
2. The Logging Level determines the amount and type of data that are logged on the Server. This setting should not be altered unless directed to do so by Eaton personnel.
3. Normally, the Foreseer Server runs as a Service and, by default, uses the local system account (User Name and Password) for access functions. In this case, the User Name should remain blank. If you wish to enable the Server to run as a specific User, enter the appropriate User Name, Password and Domain information.
4. The Startup Delay provides a time to wait, in seconds, before the Foreseer Server itself starts.
5. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those **Server Properties**.

Server Properties - Remote

The **Server Properties** dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **Remote Properties** allow the Server application and operating system to be rebooted from a Foreseer Client. Software upgrades and Device Driver uploads also can be performed from an authorized Client. Click on other tabs to present those **Server Properties**.



The following options are used for Remote Administration. The user must have Administration privileges to use these options if they are enabled.

☑ Allow Remote Restart of the Application (this program).

If the following option is enabled, make sure that the Remote Application will start automatically when the system is restarted.

☑ Allow Remote Restart of the Operating System on this computer.

If the following option is enabled, a Remote Administration program can upload files to the Remote and by using the Restart Remote Application command cause the Remote to be upgraded.

☑ Allow Remote Upgrade of the Remote Application and Device Drivers

To specify Remote Server Properties:

> ✓ Administrative Authorization is required to access **Server Properties**.

1. Select Server Properties... in the Administration menu.
2. Click on the **Remote** tab to display those **Server Properties**. Remote Server settings, by default, are enabled as indicated by the associated checkbox. Modifying any of the following remote settings requires Server Administration permission on the accessing Client.

   Allow Remote Restart of the Server Application permits connected Clients to restart the Foreseer application on this Server.

   Allow Remote Restart of the Operating System on this computer permits connected Clients to remotely perform a complete reboot of the Foreseer Server computer.

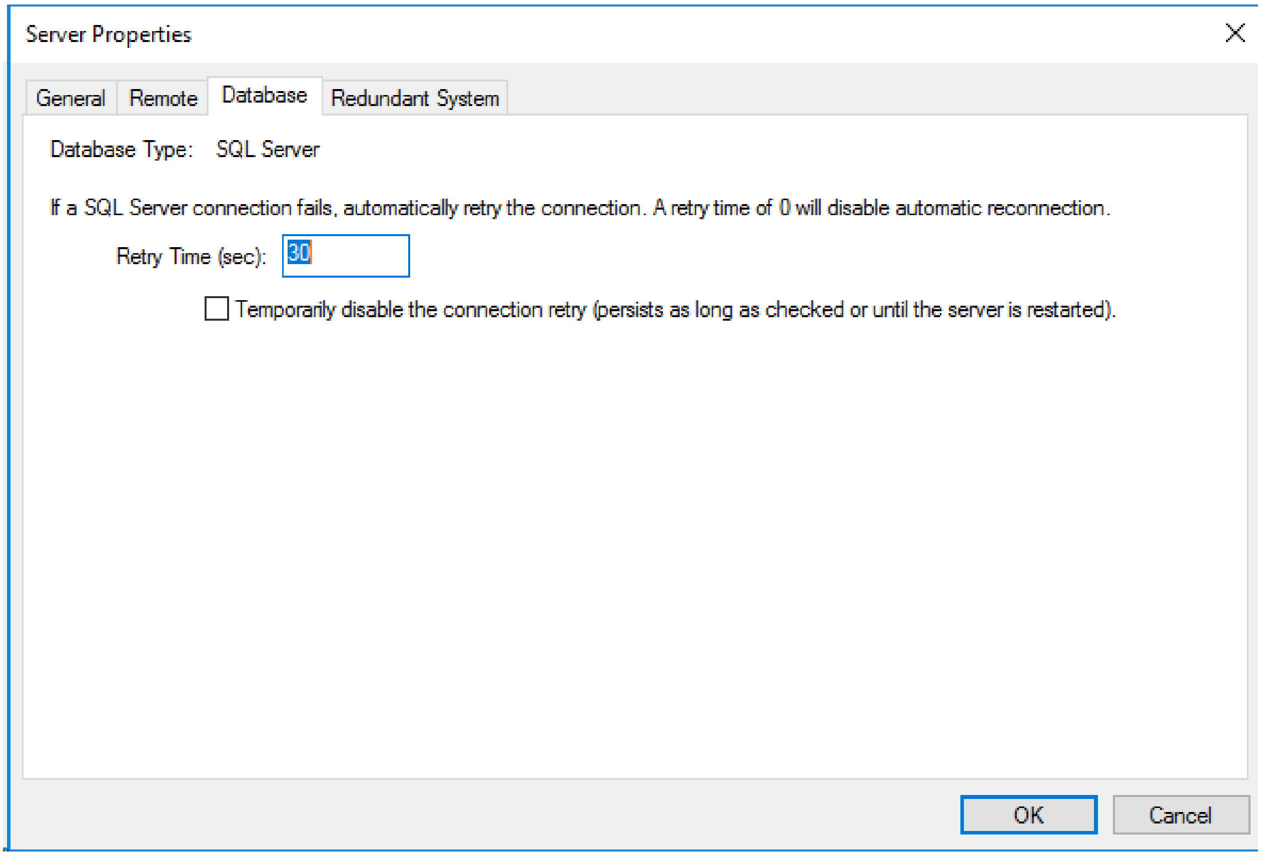
> ✓ This operating system restart should be disabled on Foreseer Servers where Auto-login is not used.

   Allow Remote Upgrade of the Server Application and Device Drivers permits authorized Clients to upload newer releases of Foreseer software and Device Drivers to the Server.

3. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those **Server Properties**.

Server Properties - Database

The Server Properties dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **Database Properties** determine historic database settings. Clicking other tabs presents those **Server Properties**.



Server Properties

Database Type: SQL Server

If a SQL Server connection fails, automatically retry the connection. A retry time of 0 will disable automatic reconnection.

Retry Time (sec): 30

□ Temporarily disable the connection retry (persists as long as checked or until the server is restarted).

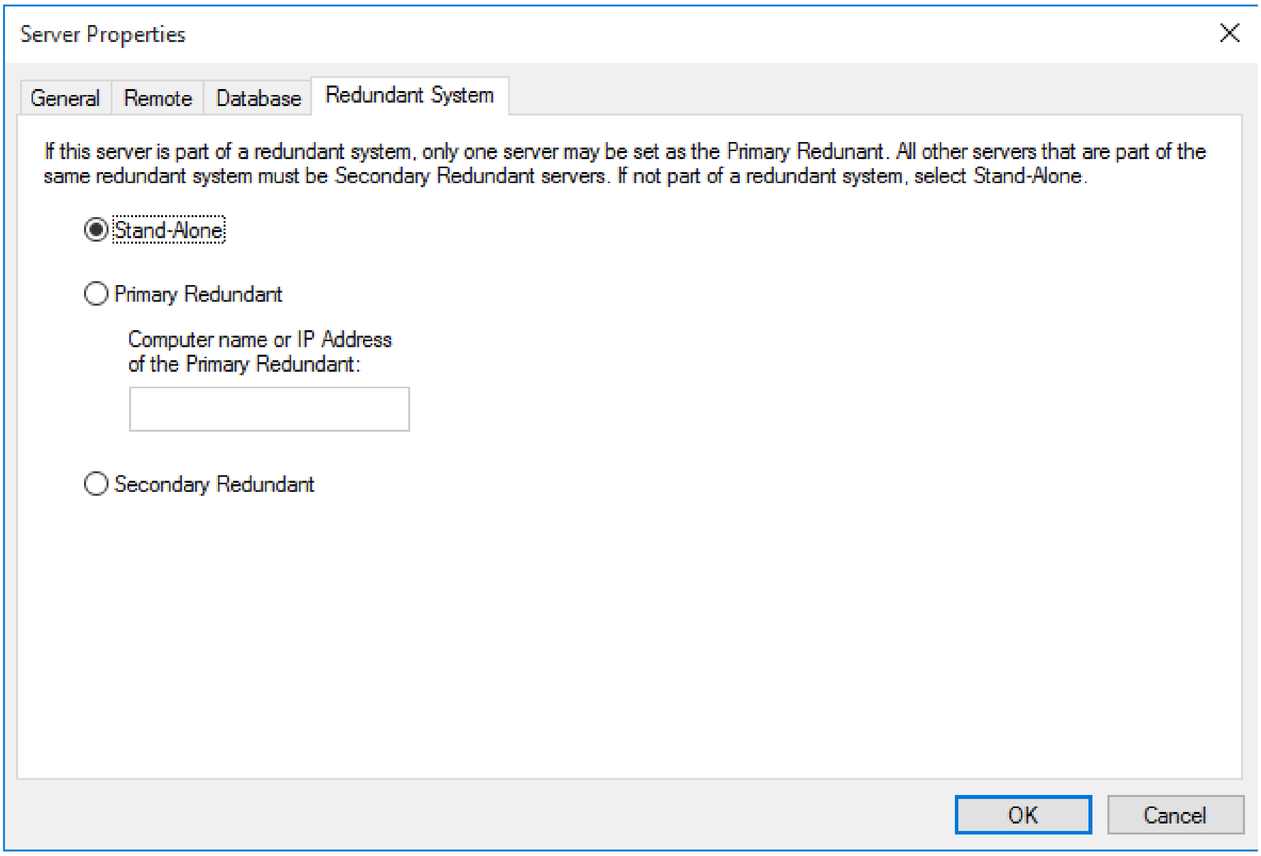
To specify Database Server Properties:

✓ Administrative Authorization is required to access **Server Properties**.

1. Select Server Properties...in the Administration menu.
2. Click the **Database** tab to display those **SQL Server Properties**. The dialog box initially identifies the Type of database. The Database Server Name identifies a remote SQL Database Server whenever it is reported, such as in Message Management, Report titles and for Heartbeat functions. The Name can be a maximum of 29 characters, but the field should remain blank if a local SQL Database Server is being used.
3. Specify the time (in seconds) between retries if connection with the remote SQL Server is lost. Setting the Retry Time to "0" disables this feature. With a Retry Time entered, you can also check the "Temporarily disable the connection retry..." box to manually suspend operation of this automatic feature, if desired, for maintenance or other reasons.
4. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those **Server Properties**.

Server Properties - Redundant System

The **Server Properties** dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **Redundant Properties** identify the Server as a backup to endure continued site monitoring in the event the principle Server fails. Click on other tabs to present those **Server Properties**.



If this server is part of a redundant system, only one server may be set as the Primary Redunant. All other servers that are part of the same redundant system must be Secondary Redundant servers. If not part of a redundant system, select Stand-Alone.

● Stand-Alone

○ Primary Redundant

Computer name or IP Address of the Primary Redundant:

○ Secondary Redundant

To specify Redundant System Properties:

Administrative Authorization is required to access **Server Properties**.

1. Select Server Properties... in the Administration menu.
2. Click on the **Redundant System** tab to display those **Server Properties** and specify the type:

   Stand-Alone is for applications where a single redundant Server is being employed.

   Primary and Secondary Redundant are used in instances where there is more than one backup Server being maintained as part of a redundancy system. Only one Server may be specified as the Primary Redundant Server and its Computer name or IP Address must be entered to identify it to the Secondary Redundant Server(s).

You cannot use LocalHost or 127.0.0.1 in Computer name or IP Address field

3. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those **Server Properties**.

Configuration Menu

The **Configuration** menu is used to alter the "shape" of the Server. Functions include modifications like remote Server management as well as adding and deleting Devices and channels. Any grayed commands cannot be performed on the selected item or within the active window.

✓ Administrative Authorization is required before proceeding with any of these commands.

The **Configuration** menu offers the following Foreseer commands:

Start Server Configuration initiates changes on the Foreseer Server. The Server Configuration Mode System Channel turns yellow and

"********SERVER CONFIGURATION MODE********"

is displayed in the window's title bar to confirm edit status.

End Server Configuration terminates changes to the Foreseer Server and returns to normal operation.

Configuration Backup... displays the Configuration Backup dialog box, allowing the Foreseer Server configuration to be saved as an archive file.

Backup... displays the Backup dialog box, setting automatic configuration backups.

Install Device... allows you to Install Devices on the Foreseer Server so that they may be monitored and added to the WebViews.

Install Devices from List... allows you to Install Multiple Devices through a .CSV file on the Foreseer Server so that they may be monitored and added to the WebViews **Views**.

Add User-Defined Channel...permits the User to create new Derived Channel.

Add Channel... permits the User to create a new Meters(Analog) or Status(Digital) Channel. This command is not available for all Devices.

Disable suspends all data archiving to the Foreseer Server for the selected Device or channel. Disabling is useful when making repairs to avoid archiving inappropriate readings and is necessary in order to Delete or Rename the Device or channel.

Enable resumes data archiving for the selected Device(s) or channel(s).

Disarm stops testing the channel values against specified alarm limits, preventing alarms from being issued.

Rearm resumes testing channel values against alarm limits.

Delete permanently deletes the selected Remote Server, Device or Channel from the configuration. Once removed, its archived information is no longer available. Deleting a Device or Channel should be done with discretion as removing it can have an adverse effect on Foreseer WebViews configurations.

Rename permits the selected Device or Channel to be renamed in response to changing conditions. It should be noted that renaming a Device or Channel should be done with discretion as changing a name can have an adverse effect on Foreseer WebViews configurations.

Copy Channel Properties copies all the currently selected channel's **Properties** to the Windows clipboard, allowing its settings to be pasted directly into another channel as its operational parameters. This command is useful when applied to an entire Device (rather than individual channels) for quickly setting up multiple Devices that contain similar channels. In either case, the channel or Device being copied **must be of the exact same type** as the one the **Properties** are being pasted into.

Paste Channel Properties pastes the previously copied **Properties** into the currently selected channel as its operational parameters. It also is useful when duplicating numerous channel settings on multiple Devices. In either case, the channel or Device being pasted into **must be of the exact same type** as the one the **Properties** are being copied from. these settings then can be individually modified as necessary. If copying from a Device (rather than a single channel), only those channels with the same Name will have their **Properties** pasted.

Create .VI File generates .VI (Device Driver) template based on the selected Device's settings. This file template can then be used to define other similar Devices.

Create All .VI Files generates .VI (Device Driver) templates for all Devices on the selected Server. These file templates can then be used to define other similar Devices.

Refresh Tree forces a refresh of all devices in the tree.

Properties... displays the selected Device Properties or channel's (Meters or Status) **Properties** dialog box, allowing its parameter settings to be reviewed or altered.

- Configuration Backup
- Automatic Configuration Backups

Configuration Backup

The Server configuration can be saved in order to retain **Channel Properties** and other system settings for subsequent Foreseer sessions. It is strongly recommended this System Administration function be performed after initial system configuration as well as before and after any significant modifications (or when performing batch changes in larger configurations) to ensure maximum disaster recovery capability. The Server Configuration Mode System Channel reports when structural changes have been to the Server configuration. The Backup archive includes all Foreseer Server configuration files, which are compressed to conserve disk space.

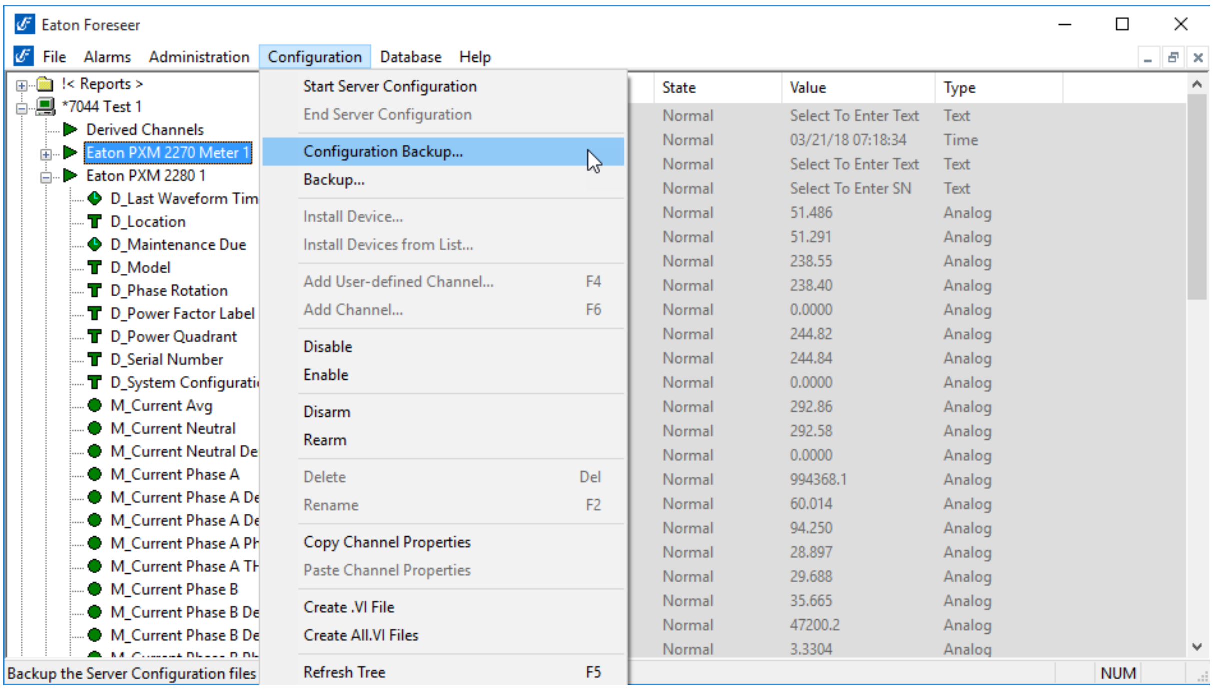
The Backup archive includes the Foreseer Server configuration data files. Data backups are NOT handled by Foreseer but by SQL Server in accordance to your corporate data backup policy.

✓ This procedure does not backup data, Log or Report files-- it is recommended that these files routinely be backed up to a network drive.

To Backup a Foreseer Server configuration:

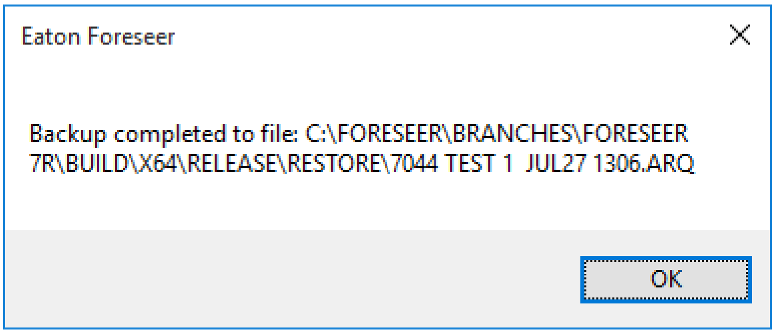
✓ Administrative Authorization is required to Backup the Server configuration.

1. Select Configuration Backup in the Configuration menu to initiate the backup.



State	Value	Type
Normal	Select To Enter Text	Text
Normal	03/21/18 07:18:34	Time
Normal	Select To Enter Text	Text
Normal	Select To Enter SN	Text
Normal	51.486	Analog
Normal	51.291	Analog
Normal	238.55	Analog
Normal	238.40	Analog
Normal	0.0000	Analog
Normal	244.82	Analog
Normal	244.84	Analog
Normal	0.0000	Analog
Normal	292.86	Analog
Normal	292.58	Analog
Normal	0.0000	Analog
Normal	994368.1	Analog
Normal	60.014	Analog
Normal	94.250	Analog
Normal	28.897	Analog
Normal	29.688	Analog
Normal	35.665	Analog
Normal	47200.2	Analog
Normal	3.3304	Analog

2. Foreseer will initiate the backup process and create a single archive file in the \ Restore\ directory of your Foreseer server installation
3. Once completed, the **Backup Completed** dialog box will display.
    1. The backup file name will be in the format:SERVERNAME MMMDD HHMM.ARQ



Backup completed to file: C:\FORESEER\BRANCHES\FORESEER 7R\BUILD\X64\RELEASE\RESTORE\7044 TEST 1 JUL27 1306.ARQ

4. Foreseer indicates when the archiving process is successfully completed. Click OK to return to the window that was active prior to the backup operation.

For Outpost Only: If an *.ARQ file is in the Config Restore folder when the Server is started, it will delete the current Data and VI folders, move the *.ARQ file into the Restore folder and restore it. This is also a new destination for the Upload Files command. It is important to remember that the restore is automatic at the next restart and that the Data and VI folder contents will be deleted.

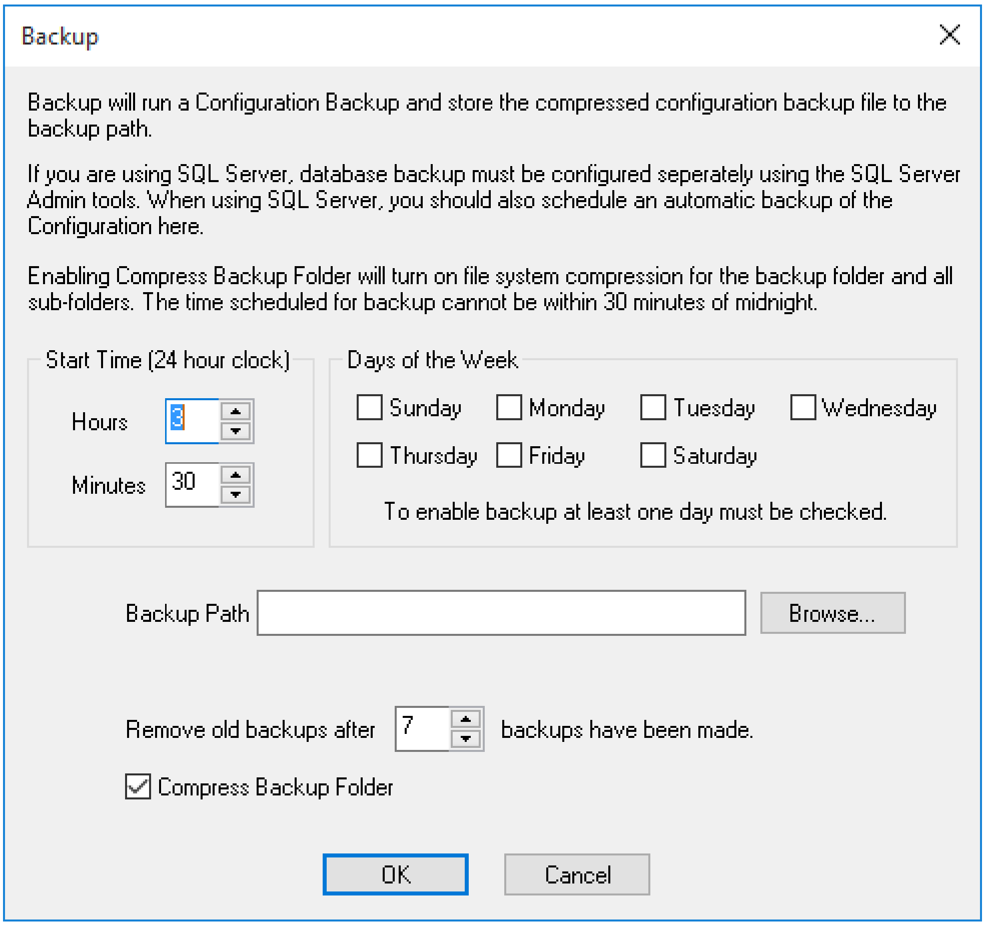
Automatic Configuration Backups

You can schedule configuration backups automatically at specified intervals. A network drive is the recommended backup destination.

Make certain that the user account used by Foreseer has Full Control permission for all the directories under the Foreseer installation directory. Otherwise, the backup process may fail.

To schedule regular backups:

1. Select Backup in the Server's Configuration menu.



Backup will run a Configuration Backup and store the compressed configuration backup file to the backup path.

If you are using SQL Server, database backup must be configured seperately using the SQL Server Admin tools. When using SQL Server, you should also schedule an automatic backup of the Configuration here.

Enabling Compress Backup Folder will turn on file system compression for the backup folder and all sub-folders. The time scheduled for backup cannot be within 30 minutes of midnight.

Start Time (24 hour clock)

Hours 3

Minutes 30

Days of the Week

□ Sunday □ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

To enable backup at least one day must be checked.

Backup Path

Remove old backups after 7 backups have been made.

☑ Compress Backup Folder

2. Specify when the backup is to be performed. The Start Time is based on a 24- hour clock: for example, 5:00 p.m. is entered as “17:00.” Note that the backup cannot occur within ten minutes of midnight and that there are restrictions based on the type of backup media. The Start Time plus the duration of the archive cannot extend through midnight if archiving to an external drive and it cannot be within the half hour preceding midnight if archiving to a remote network drive.
3. Check the Day(s) of the Week on which the backup is performed. Daily backups are strongly encouraged and recommended.
4. Enter or browse to the desired backup path.
5. You can adjust the maximum number of backups that are stored in the specified path.
6. Click OK to enable the displayed Data Backup settings. Archiving will be performed automatically at the scheduled time on the selected day(s).

Database Menu

The **Database** menu is used to perform various Foreseer functions related to the databases. Any grayed commands cannot be performed.

✓ Administrative Authorization is required before proceeding with any of these commands.

The **Database** menu offers the following Foreseer commands:

- Start Database Session - initiates data acquisition from the connected equipment by the Foreseer Server.
- End Database Session - suspends data acquisition from the connected equipment by the Foreseer Server.
- Check Databases - verifies the integrity of the Foreseer Server databases in the event the program was terminated improperly.
- Fix Databases - corrects any problems detected during the Check Databases process.
- SQL Server Properties - launches the SQL Server Setup dialog box.

- Database SQL

Database SQL

✓ The Windows service account of SQL user leveraged by Foreseer must be assigned the following SQL Server roles:

- public
- bulkadmin
- dbcreator

In addition to the above roles, there are times when a Database Consistency Check may need to be executed. In order to run DBCC, the account must also contain the following user mapping to the master db:

- public
- dbbackupoperator

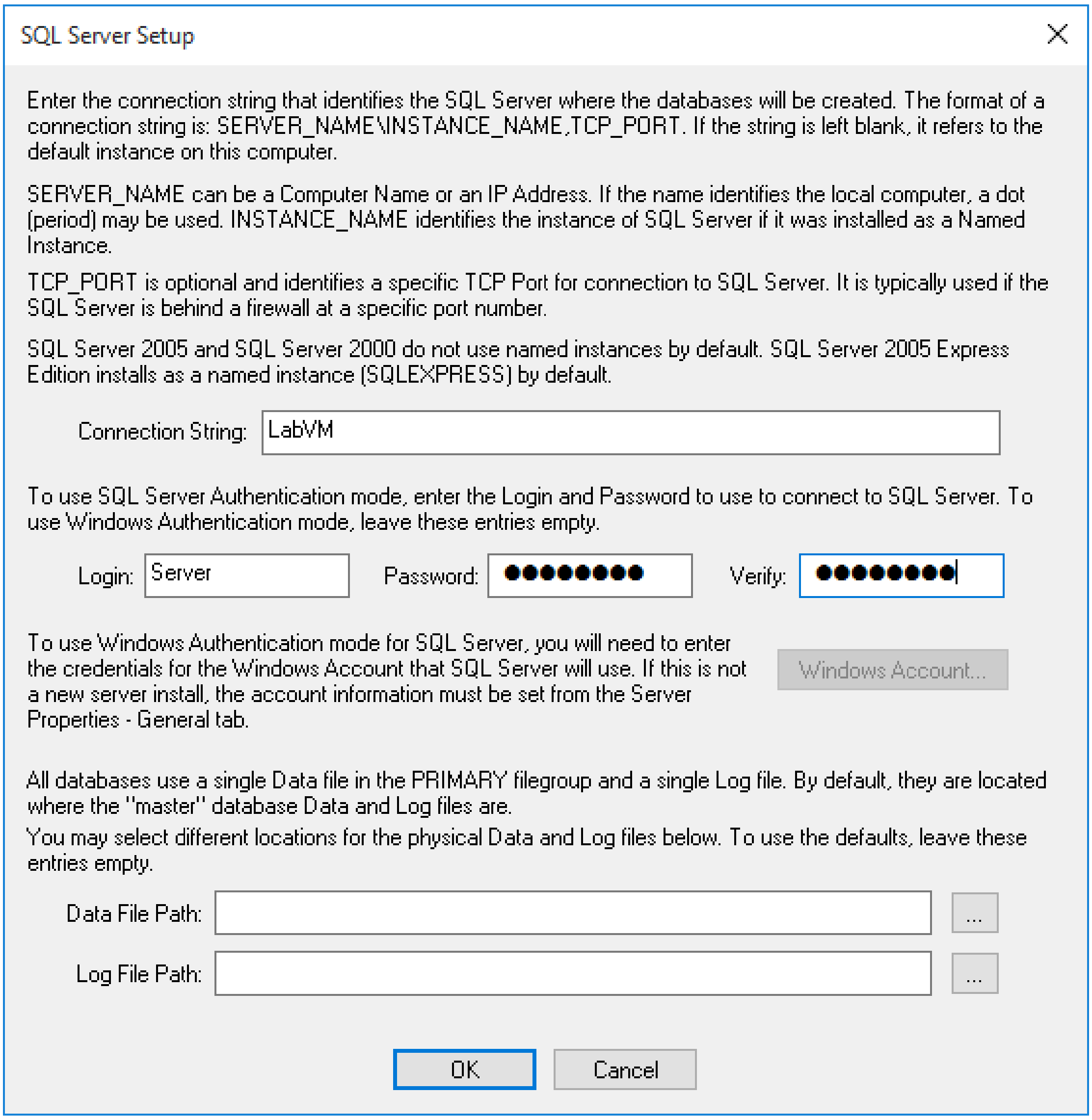
Contact your Database Administrator for assistance with provisioning of these entitlements to the account used by Foreseer.

Use this dialog box to configure access to your instance of SQL Server. Follow the instructions on the dialog box to configure the connection string.

You can choose to use either an account managed by SQL Server or a Windows account. If you plan to use a SQL-user, fill in the username and password credentials. If you plan to use Windows Authentication as part of a service account, leave these fields blank.

If this isn't a new server installation, you'll need to set the account information in the Server Properties dialog box (General tab).

You can also change the location of the Data and Log files.



Enter the connection string that identifies the SQL Server where the databases will be created. The format of a connection string is: SERVER_NAME\INSTANCE_NAME,TCP_PORT. If the string is left blank, it refers to the default instance on this computer.

SERVER_NAME can be a Computer Name or an IP Address. If the name identifies the local computer, a dot (period) may be used. INSTANCE_NAME identifies the instance of SQL Server if it was installed as a Named Instance.

TCP_PORT is optional and identifies a specific TCP Port for connection to SQL Server. It is typically used if the SQL Server is behind a firewall at a specific port number.

SQL Server 2005 and SQL Server 2000 do not use named instances by default. SQL Server 2005 Express Edition installs as a named instance (SQLEXPRESS) by default.

Connection String: LabVM

To use SQL Server Authentication mode, enter the Login and Password to use to connect to SQL Server. To use Windows Authentication mode, leave these entries empty.

Login: Server Password: ●●●●●●●● Verify: ●●●●●●●●

To use Windows Authentication mode for SQL Server, you will need to enter the credentials for the Windows Account that SQL Server will use. If this is not a new server install, the account information must be set from the Server Properties - General tab.

All databases use a single Data file in the PRIMARY filegroup and a single Log file. By default, they are located where the "master" database Data and Log files are.

You may select different locations for the physical Data and Log files below. To use the defaults, leave these entries empty.

Data File Path:

Log File Path:

Installing Devices

You can add new equipment to the Foreseer Server using either a step-by-step installation procedure (outlined in this topic) or by loading a .csv file that contains information about a list of devices. The Device Installation Wizard guides you through the procedure, prompting the necessary information and applying default parameters based on a standard list of monitored points for each Device. Individual settings for these points may be changed later (refer to Channel Properties).

- Device Installation Wizard
- Install Devices From List
- Serial Connection
- Device Channel Selection
- Deleting Devices and Channels

Device Installation Wizard

✓ You cannot install a device that has more than 1000 channels

To install a Device on the Foreseer Server:

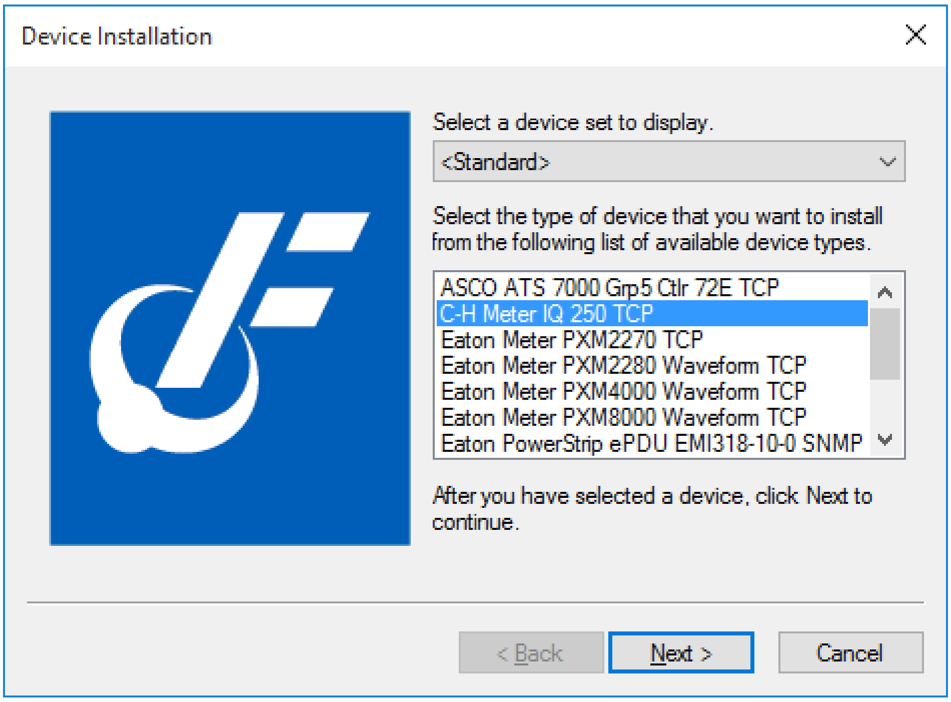
1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

   "********SERVER CONFIGURATION MODE********"

   is displayed in the Windows title bar to confirm operational status.
2. Right-click in the Tree View window and select Install New Device to access that dialog box. Locate the Configuration Checklist for the new equipment, then click Next> to continue.

✓ If the device type is not shown,contact your Foreseer sales representative to purchase the proper device driver.

3. Select the appropriate Device from the list of supported equipment and click Next>.



Device Installation

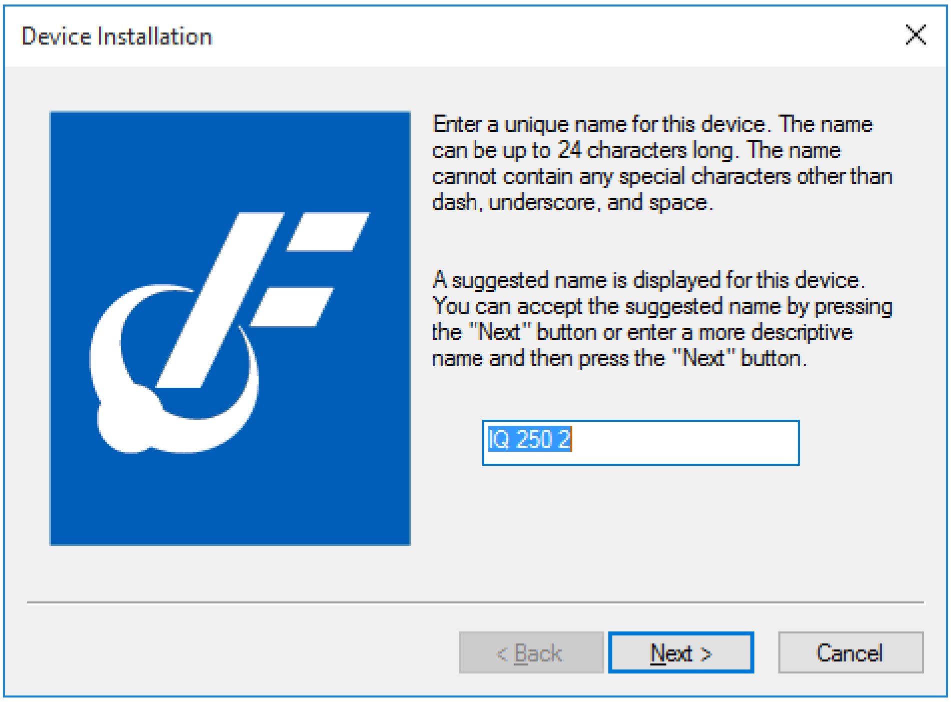
Select a device set to display.

<Standard>

Select the type of device that you want to install from the following list of available device types.

ASCO ATS 7000 Grp5 Ctlr 72E TCP
C-H Meter IQ 250 TCP
Eaton Meter PXM2270 TCP
Eaton Meter PXM2280 Waveform TCP
Eaton Meter PXM4000 Waveform TCP
Eaton Meter PXM8000 Waveform TCP
Eaton PowerStrip ePDU EMI318-10-0 SNMP

After you have selected a device, click Next to continue.



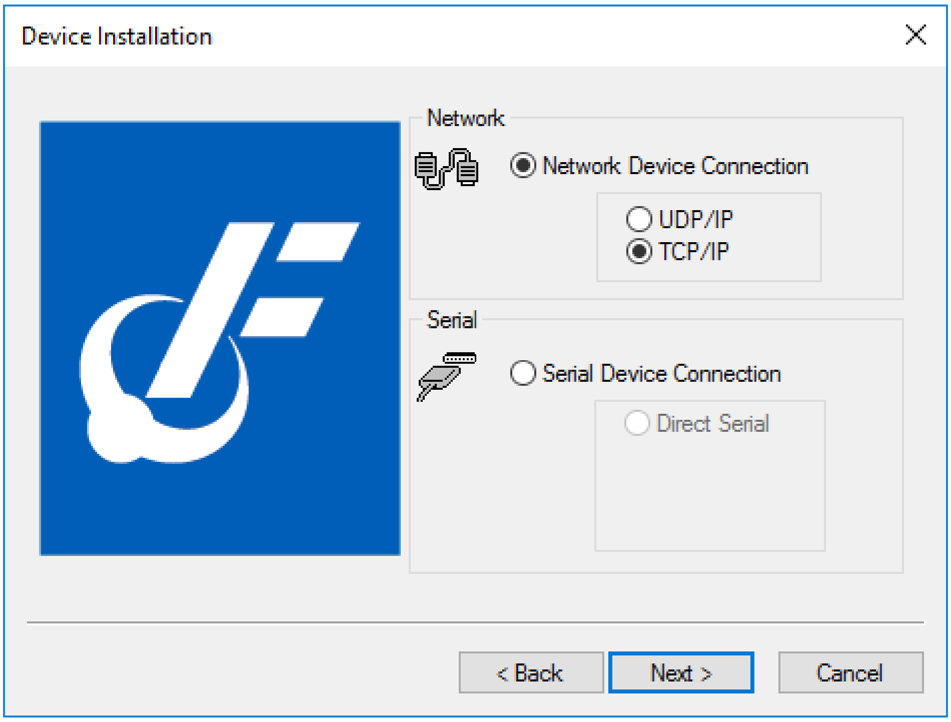
Enter a unique name for this device. The name can be up to 24 characters long. The name cannot contain any special characters other than dash, underscore, and space.

A suggested name is displayed for this device. You can accept the suggested name by pressing the "Next" button or enter a more descriptive name and then press the "Next" button.

IQ 250 2

✓ TCP/IP protocol must be installed on the Server PC regardless of the type of Device connection.

4. Accept the suggested Name for the Device, or enter another unique description, up to 24 characters, then click Next > to continue. Note that “_” and “-” are the only non-alphanumeric characters allowed in the name.
5. Specify whether the interface between the Server and the Device is a Network or a Serial Connection, as well as the appropriate type, and click Next>.



Device Installation

Network

● Network Device Connection

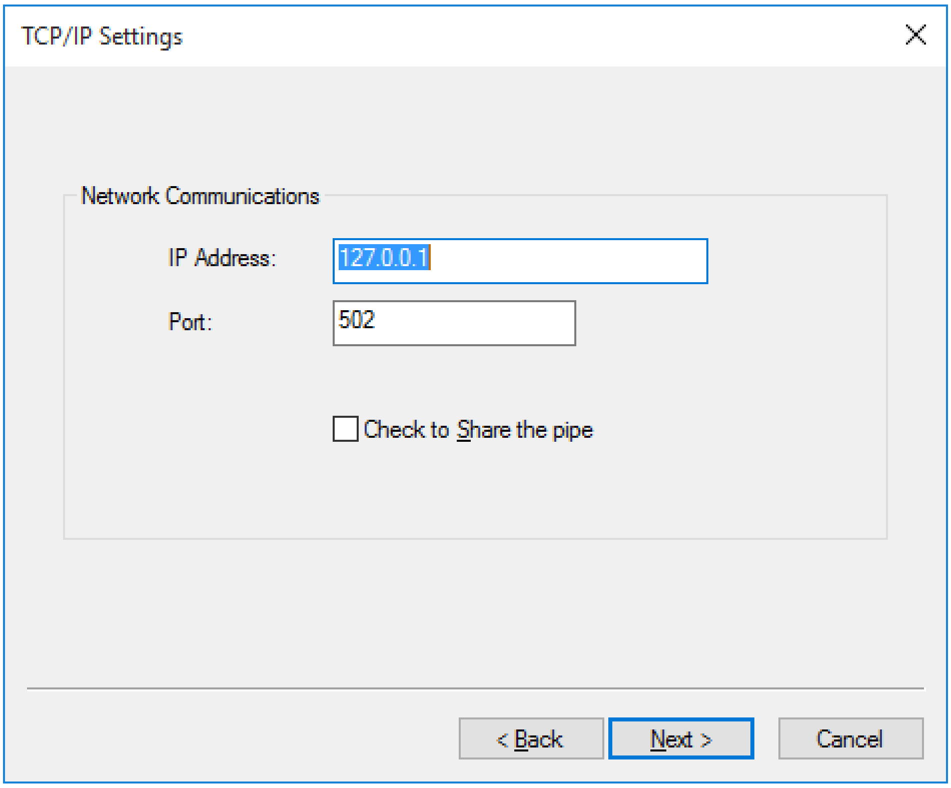
○ UDP/IP

● TCP/IP

Serial

○ Serial Device Connection

○ Direct Serial



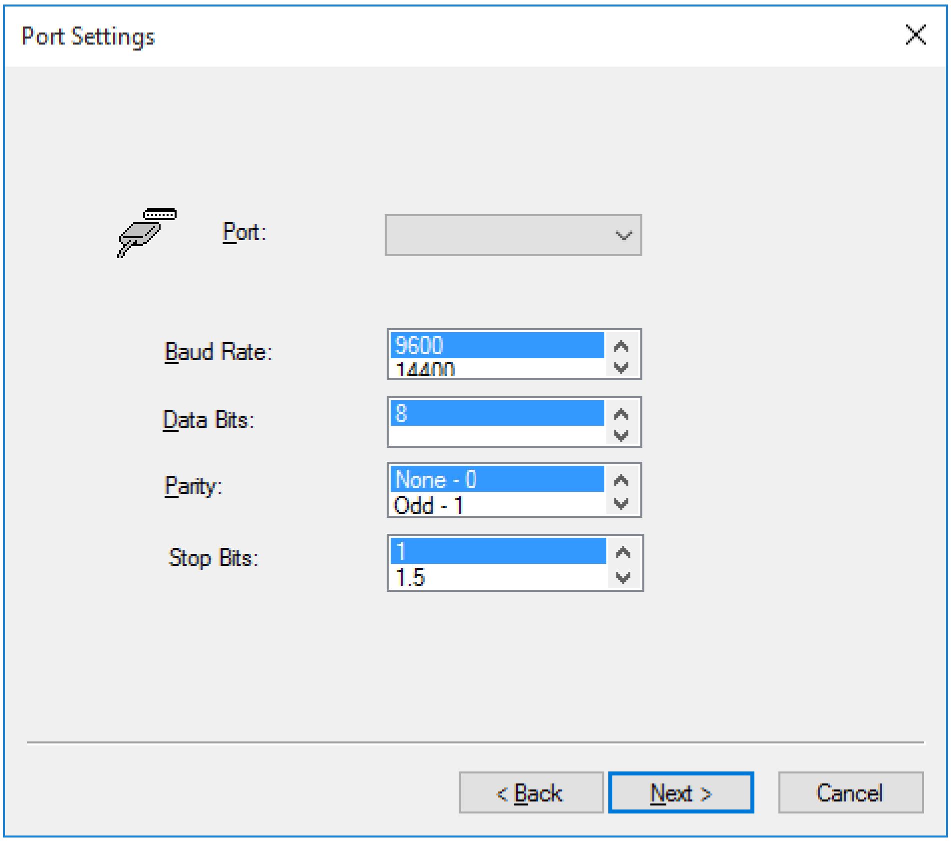
TCP/IP Settings

Network Communications

IP Address: 127.0.0.1

Port: 502

□ Check to Share the pipe


Port Settings

Port:

Baud Rate: 9600

Data Bits: 8

Parity: None - 0

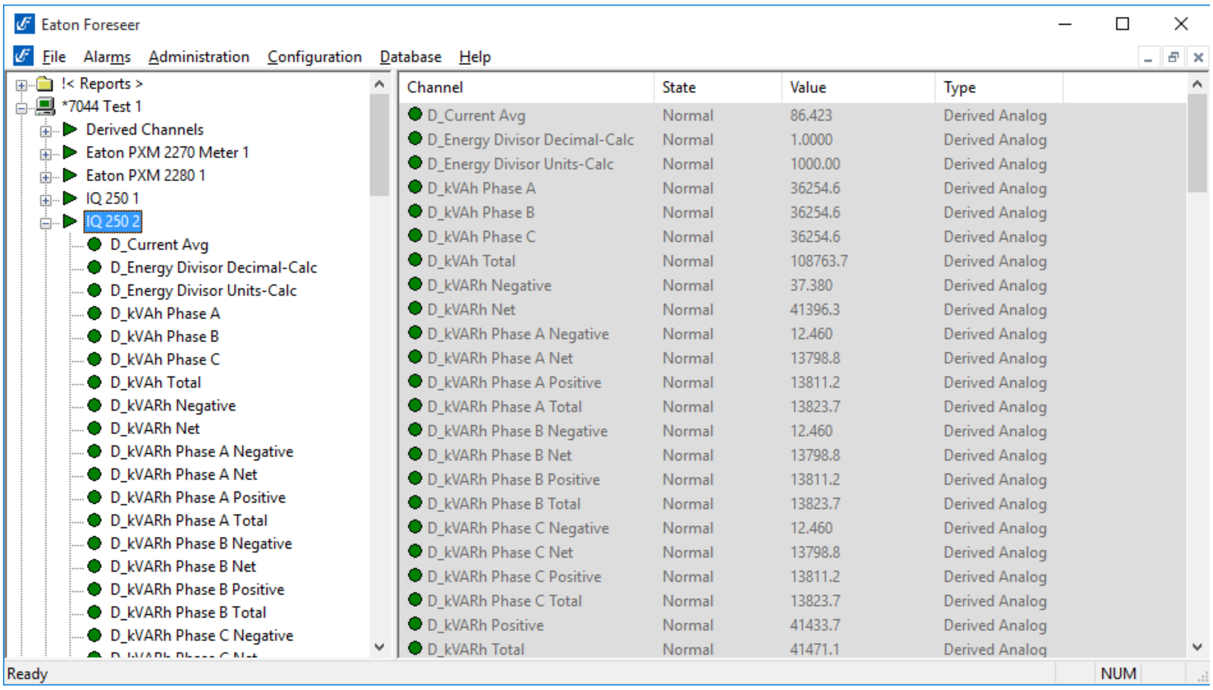
Stop Bits: 1

6. Enter the necessary Device Connection information:
7. For a Network Device, enter its IP Address or URL/Web address. This Address must be correct, or the Server will be unable to communicate with the target equipment. Click OK to accept the entry and return to the Device Installation Wizard window.
8. Selecting Serial Connection prompts additional interface information. A Direct Serial Connection requires that you specify the COM Port to which the Device is connected and its communications settings. Accept the displayed serial Port or assign another from the drop down list of selections in the Serial Communications Port field.
9. Press the Settings button to display the Port's Properties dialog box containing additional serial interface parameters. Click OK to enable the displayed parameters and return to the Device Installation Wizard window.
10. Once the Device connection is properly configured, click Next> and Foreseer will attempt to establish connections with the specified equipment.

> ⓘ If the device does not communicate it will not be installed.

11. Verify that the information displayed about the Device corresponds to the information recorded on your Configuration Checklist. If not, Cancel the installation and recheck the Device. With the correct Device information displayed, click Next>.
12. With the target Device and the interface connection defined, click Finish to complete the installation. The new equipment will appear in the Devices window. Install any additional Devices, if necessary, using the same procedure for each.

If installation is unsuccessful or the Device information does not appear in the Identification window, go <Back and check that all configuration entries are proper and that hardware connections with the equipment are correct. After verifying the configuration and connections, once again attempt to install the Device. Contact Eaton Corporation - Foreseer Technical Support if Device installation problems persist.



- !< Reports >
- *7044 Test 1
  - Derived Channels
  - Eaton PXM 2270 Meter 1
  - Eaton PXM 2280 1
  - IQ 250 1
  - IQ 250 2
    - D_Current Avg
    - D_Energy Divisor Decimal-Calc
    - D_Energy Divisor Units-Calc
    - D_kVAh Phase A
    - D_kVAh Phase B
    - D_kVAh Phase C
    - D_kVAh Total
    - D_kVARh Negative
    - D_kVARh Net
    - D_kVARh Phase A Negative
    - D_kVARh Phase A Net
    - D_kVARh Phase A Positive
    - D_kVARh Phase A Total
    - D_kVARh Phase B Negative
    - D_kVARh Phase B Net
    - D_kVARh Phase B Positive
    - D_kVARh Phase B Total
    - D_kVARh Phase C Negative
    - D_kVARh Phase C Net

Channel	State	Value	Type
● D_Current Avg	Normal	86.423	Derived Analog
● D_Energy Divisor Decimal-Calc	Normal	1.0000	Derived Analog
● D_Energy Divisor Units-Calc	Normal	1000.00	Derived Analog
● D_kVAh Phase A	Normal	36254.6	Derived Analog
● D_kVAh Phase B	Normal	36254.6	Derived Analog
● D_kVAh Phase C	Normal	36254.6	Derived Analog
● D_kVAh Total	Normal	108763.7	Derived Analog
● D_kVARh Negative	Normal	37.380	Derived Analog
● D_kVARh Net	Normal	41396.3	Derived Analog
● D_kVARh Phase A Negative	Normal	12.460	Derived Analog
● D_kVARh Phase A Net	Normal	13798.8	Derived Analog
● D_kVARh Phase A Positive	Normal	13811.2	Derived Analog
● D_kVARh Phase A Total	Normal	13823.7	Derived Analog
● D_kVARh Phase B Negative	Normal	12.460	Derived Analog
● D_kVARh Phase B Net	Normal	13798.8	Derived Analog
● D_kVARh Phase B Positive	Normal	13811.2	Derived Analog
● D_kVARh Phase B Total	Normal	13823.7	Derived Analog
● D_kVARh Phase C Negative	Normal	12.460	Derived Analog
● D_kVARh Phase C Net	Normal	13798.8	Derived Analog
● D_kVARh Phase C Positive	Normal	13811.2	Derived Analog
● D_kVARh Phase C Total	Normal	13823.7	Derived Analog
● D_kVARh Positive	Normal	41433.7	Derived Analog
● D_kVARh Total	Normal	41471.1	Derived Analog

13. With all Devices properly installed, click No to terminate the installation process. You may wish to select newly installed equipment in the Server's Tree View and review the default settings assigned to each of its input channels. The Properties vary slightly depending on whether it is a Meter (analog) or Status (digital) channel and they only can be changed by a User with Administrative authorization. Refer to Channel Properties for more information on these data point settings.
14. End Server Configuration mode

It is advisable to end and restart Server Config Mode when installing >10-15 devices to allow the database to be synchronized to the changes.

Do this after every block of 10-15 devices.

Install Devices From List

Before adding devices in any manner it is highly recommended to take a configuration backup (ARQ) so you can return to a previous point if issues are encountered.

As an alternative to loading a single device via the wizard, you can load a set of devices by predefining these in a comma-separated values (CSV) file. This “device list” file has the following format:

device_name,vi_file_name,IP_address,port_number,driver_specific_info

Where:

device_name is the name that will be used in Foreseer for the device.

vi_file_name is the filename of the driver file for that device. This file is stored in the install_path/Foreseer/vifolder. Note that some driver file names may have a single comma. Foreseer will handle thiscorrectly.

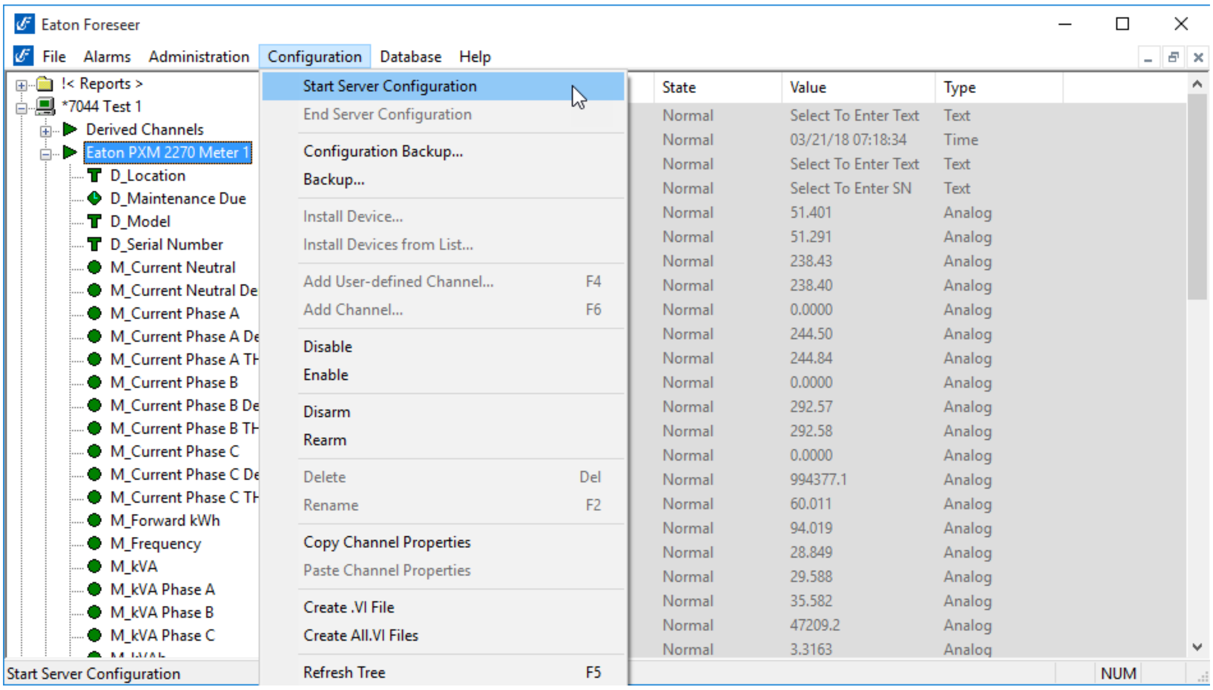
IP_address is the IP address for that device. Set this to nonefor the Nothing driver.

port_number is the port portion of the device address. Leave this field blank for the Nothing driver. You may also leave this field blank to use the default port for that specific device protocol or enter a valid port number.

driver_specific_info is either the device ID (for Modbus) or the read community string for SNMP. Set this to nonefor the Nothing driver.

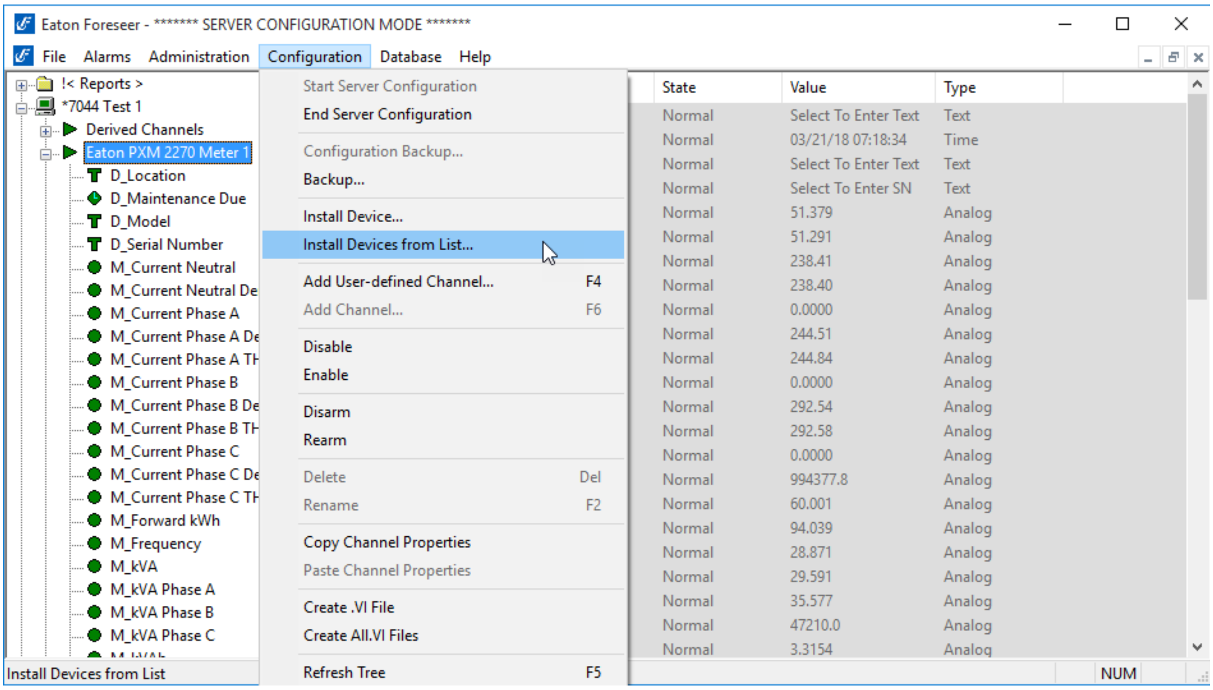
To add a device from the using the device list file:

1. In the Configuration menu, click Start Server Configuration.



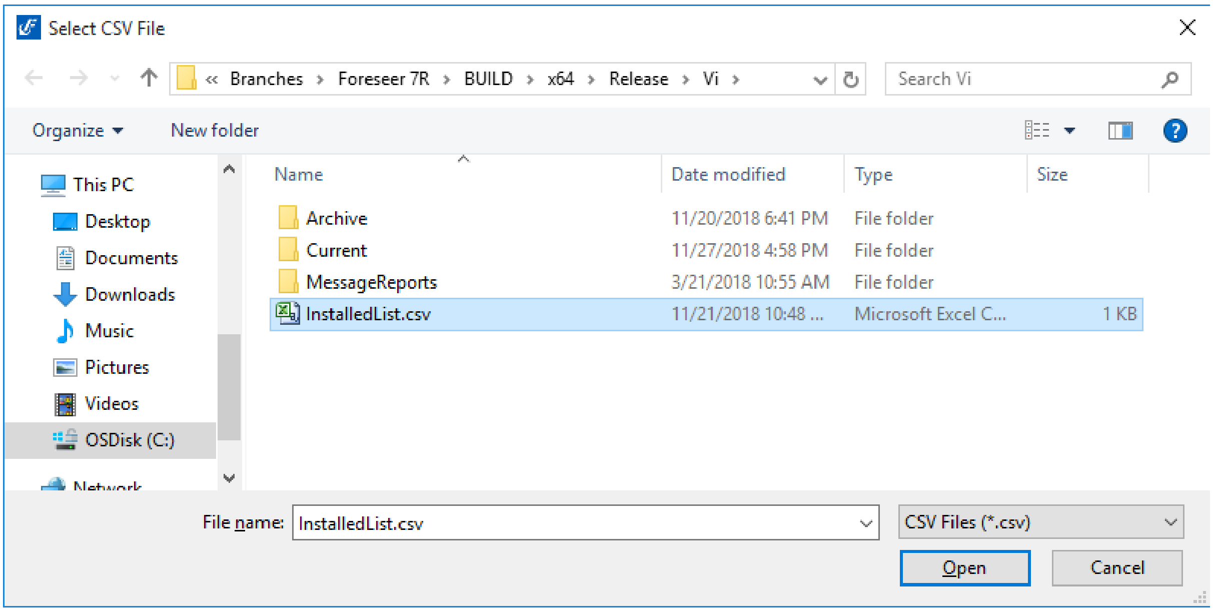
State	Value	Type
Normal	Select To Enter Text	Text
Normal	03/21/18 07:18:34	Time
Normal	Select To Enter Text	Text
Normal	Select To Enter SN	Text
Normal	51.401	Analog
Normal	51.291	Analog
Normal	238.43	Analog
Normal	238.40	Analog
Normal	0.0000	Analog
Normal	244.50	Analog
Normal	244.84	Analog
Normal	0.0000	Analog
Normal	292.57	Analog
Normal	292.58	Analog
Normal	0.0000	Analog
Normal	994377.1	Analog
Normal	60.011	Analog
Normal	94.019	Analog
Normal	28.849	Analog
Normal	29.588	Analog
Normal	35.582	Analog
Normal	47209.2	Analog
Normal	3.3163	Analog

2. In the Configuration menu, click Install Devices from List.



State	Value	Type
Normal	Select To Enter Text	Text
Normal	03/21/18 07:18:34	Time
Normal	Select To Enter Text	Text
Normal	Select To Enter SN	Text
Normal	51.379	Analog
Normal	51.291	Analog
Normal	238.41	Analog
Normal	238.40	Analog
Normal	0.0000	Analog
Normal	244.51	Analog
Normal	244.84	Analog
Normal	0.0000	Analog
Normal	292.54	Analog
Normal	292.58	Analog
Normal	0.0000	Analog
Normal	994377.8	Analog
Normal	60.001	Analog
Normal	94.039	Analog
Normal	28.871	Analog
Normal	29.591	Analog
Normal	35.577	Analog
Normal	47210.0	Analog
Normal	3.3154	Analog

3. In the Select CSV File dialog box, browse to the CSV file.
4. Click Open.



Name	Date modified	Type	Size
Archive	11/20/2018 6:41 PM	File folder	
Current	11/27/2018 4:58 PM	File folder	
MessageReports	3/21/2018 10:55 AM	File folder	
InstalledList.csv	11/21/2018 10:48 ...	Microsoft Excel C...	1 KB

File name: InstalledList.csv

5. End Server Configuration

Drivers known at this time that can be installed using the Install from List feature include:

- 6-Modbus3
- 6-SNMPManger3
- 6-PowerXpertMeter
- 6-CyberScience CyTime SER

- 6-SquareD_PM800
- 6-PowerXpertMeter2200

This feature is limited to only 15 devices at a time.

Examples:

Modbus device installs:

PX Meter 1, 7-PowerXpert Meter 4000 TCP.vi, 10.22.50.30, 502,1
PX Meter 2, 7-PowerXpert Meter 150 TCP.vi, 10.22.50.50, 951,1

SNMP device installs:

PW 5125 1, 7-Powerware UPS 5125 SNMP.vi, 10.22.50.32, 161,public
PW 5125 2, 7-Powerware UPS 9395 SNMP.vi, 10.22.50.75, ,public

Nothing device installs:

Nothing 1, 7-Nothing.vi, none

You can load the .csv file into Foreseer through any of the following methods:

- The Foreseer Web Configuration Utility
- Use the Upload Files feature of Web Configuration.
    - These files should be uploaded to the Server/Vi location.
- The Foreseer Server.

The file will be processed and validated. If no errors are found, the devices will be added to the Foreseer system configuration. Should errors be detected in the device list file, refer to the error dialog boxes and the log report.

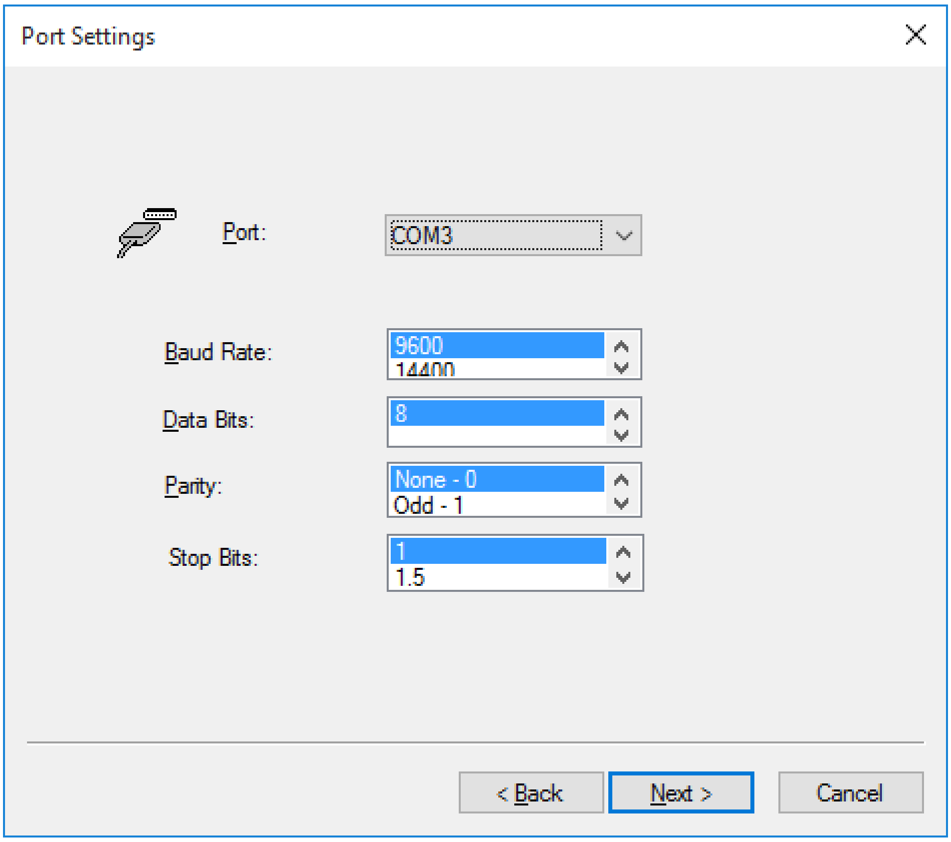
> ✓ After adding all the devices to your Foreseer Server, you should run a System Configuration Report. You should maintain an inventory of all the components in a way you uniquely identify each component. The System Configuration Report provides information about devices including IP address and Ports.

Serial Connection

The Device's **Port Settings** must be specified if a Direct Serial or VIM II connection is used. Either choice requires that you specify the Serial Communications Port and its settings.

To configure a Direct Serial Connection at the Foreseer Server:

1. Accept the displayed Port or assign another one if necessary. Click on the associated arrow to display a drop list of those Ports currently available.



Port Settings

Port: COM3

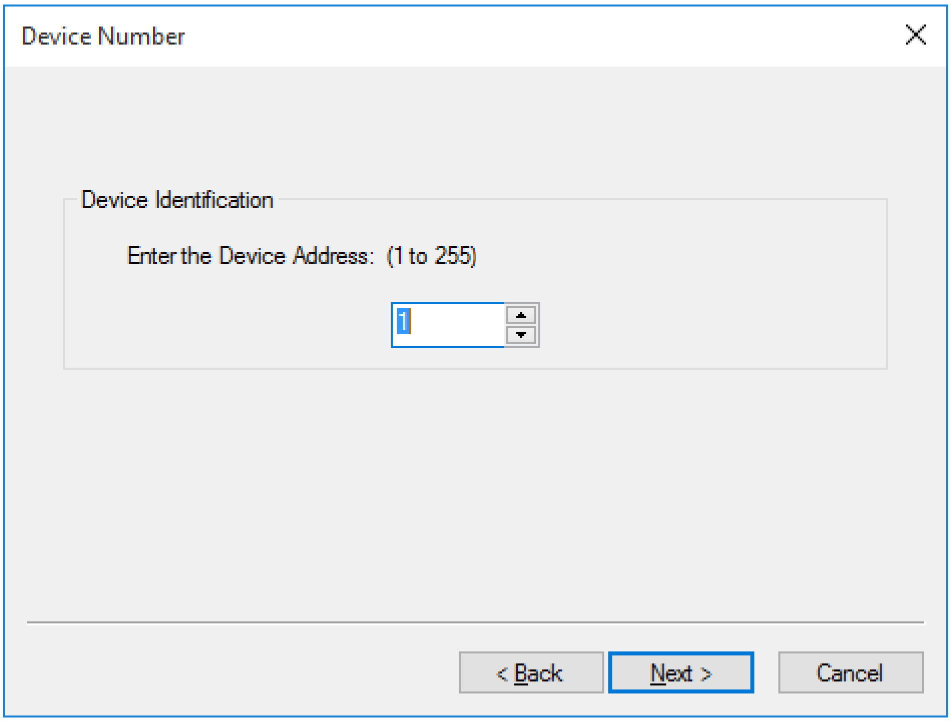
Baud Rate: 9600

Data Bits: 8

Parity: None - 0

Stop Bits: 1

2. Press the Next button to display the Device Number dialog



Device Number

Device Identification

Enter the Device Address: (1 to 255) 1

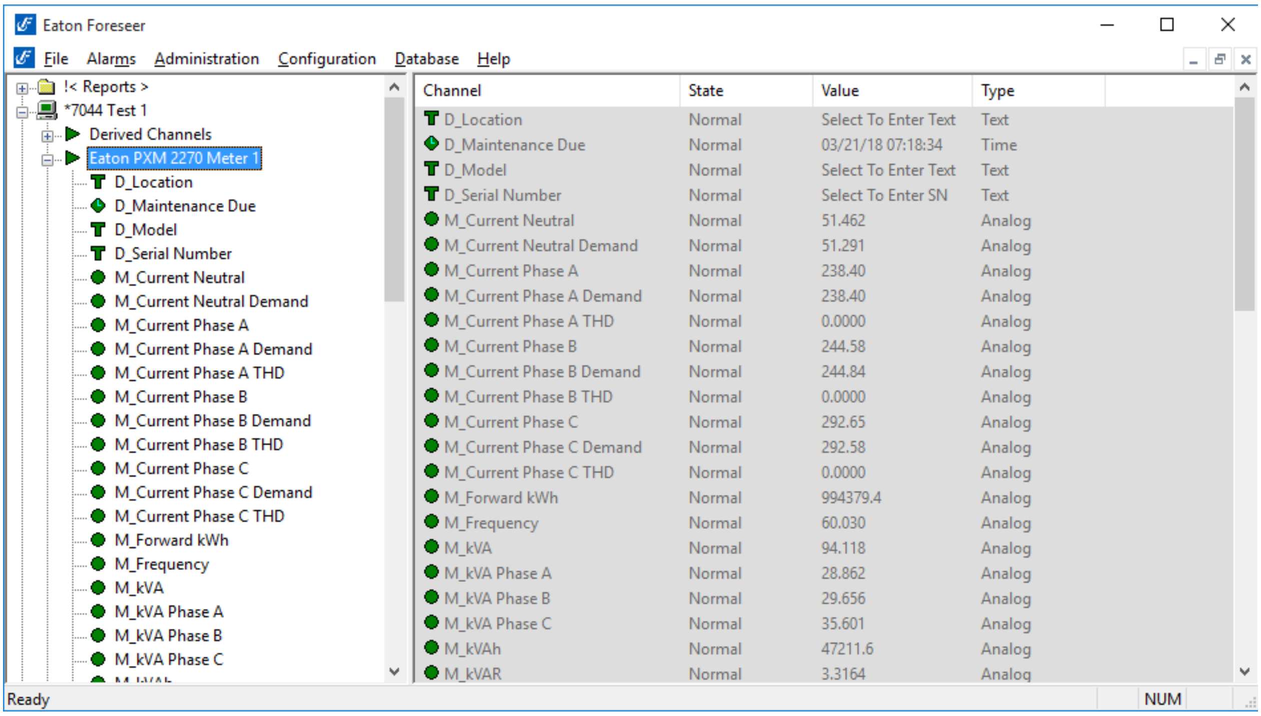
3. Press the Next button to enable the displayed Port Settings and return to the **Device**

Installation Wizard.

The process for entering the necessary configuration settings for a VIM II Direct Serial Connection is similar. After specifying the communicationsPort and Device Settings for the VIM II, you are prompted to specify the VIM II Address and Port. Click OK to enable the displayed parameters and return to the **Device Installation Wizard**.

Device Channel Selection

The **Device/Channel Selection** dialog box is used in configuring several Foreseer functions. Listed Devices and channels are referenced to their respective Servers and must exist there to be available for selection. Clicking on the "**+**" preceding a Device icon expands its list of configured channels; selecting a channel highlights it.



Channel	State	Value	Type
D_Location	Normal	Select To Enter Text	Text
D_Maintenance Due	Normal	03/21/18 07:18:34	Time
D_Model	Normal	Select To Enter Text	Text
D_Serial Number	Normal	Select To Enter SN	Text
M_Current Neutral	Normal	51.462	Analog
M_Current Neutral Demand	Normal	51.291	Analog
M_Current Phase A	Normal	238.40	Analog
M_Current Phase A Demand	Normal	238.40	Analog
M_Current Phase A THD	Normal	0.0000	Analog
M_Current Phase B	Normal	244.58	Analog
M_Current Phase B Demand	Normal	244.84	Analog
M_Current Phase B THD	Normal	0.0000	Analog
M_Current Phase C	Normal	292.65	Analog
M_Current Phase C Demand	Normal	292.58	Analog
M_Current Phase C THD	Normal	0.0000	Analog
M_Forward kWh	Normal	994379.4	Analog
M_Frequency	Normal	60.030	Analog
M_kVA	Normal	94.118	Analog
M_kVA Phase A	Normal	28.862	Analog
M_kVA Phase B	Normal	29.656	Analog
M_kVA Phase C	Normal	35.601	Analog
M_kVAh	Normal	47211.6	Analog
M_kVAR	Normal	3.3164	Analog

Deleting Devices and Channels

Devices and channels are easily deleted from the Foreseer Server, rendering their previously archived data no longer available on the current database. In most cases, to restore a channel once it has been removed from the Server configuration, its associated Device must be deleted and re-installed before it is again available.

✓ Administrative Authorization is required to Delete Devices and Channels.

To remove a Channel from the Foreseer Server:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

   "********SERVER CONFIGURATION MODE********"

   is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired Device or channel, then right-click and choose Disable to temporarily suspend data gathering activity.
3. With the desired Device or channel highlighted, right-click to access the context-sensitive menu.
4. Choose Delete and you are cautioned that all information about the chosen component will be permanently purged from the Server.
5. Press Yes to remove the component from the Server.
6. In the case of a deleted channel, highlight the parent Device once again and choose Enable from the context-sensitive menu to restore data gathering.
7. Choose the End Server Configuration command in the Configuration menu to conclude Server configuration and restore normal Foreseer data gathering activity.

Reports

Foreseer **Reports** produce ASCII text files that furnish important insights into system performance by providing predefined information. All the archived information required to produce a **Report** already resides at the Foreseer Server and can be reviewed locally, printed and distributed to concerned departments or incorporated into other documents.

> ✓ **Reports** are created and maintained at the individual Server and cannot be modified by the Foreseer Client.

The Foreseer **Report** formats are:

Alarm History (1 Day, 7 Day, 30 Day) is a series of **Reports** listing all alarms detected over the last day, week and month. These three **Report** formats consist of all alarm conditions recorded within the respective interval. If no alarm events were detected during the period, that status condition is reported.

Alarm History Custom permits the range and content of an Alarm History Report to be specified.

Audit History Custom reports the addition and deletion of Devices and channels to the Server configuration as well as when database sessions are started and stopped.

Channel Data Report (30, 60, or 90 Day) Provides minimum, maximum, and average values for each channel from the selected device over the selected time period. This is not available in tab-delimited format.

Channel Report furnishes parameters for all channels on a Server or for a selected Device.

Driver Log File report provides detailed information on the drivers in use by the Foreseer system.

Interval Data Report furnishes historical data at intervals at different periods (1 minute, 15 minutes, etc..). While you can view the last three reports from the Foreseer Server application, generating new reports must be performed from WebViews.

Log File reports all recorded events since the last system reset.

Notes History (1 Day, 7 Day, 30 Day) reports all Notes logged over the last day, week and month.

Notes History Custom permits the range and content of a Notes History Report to be specified.

Previous Driver Log File report provides detailed information on the drivers in use by the Foreseer system.

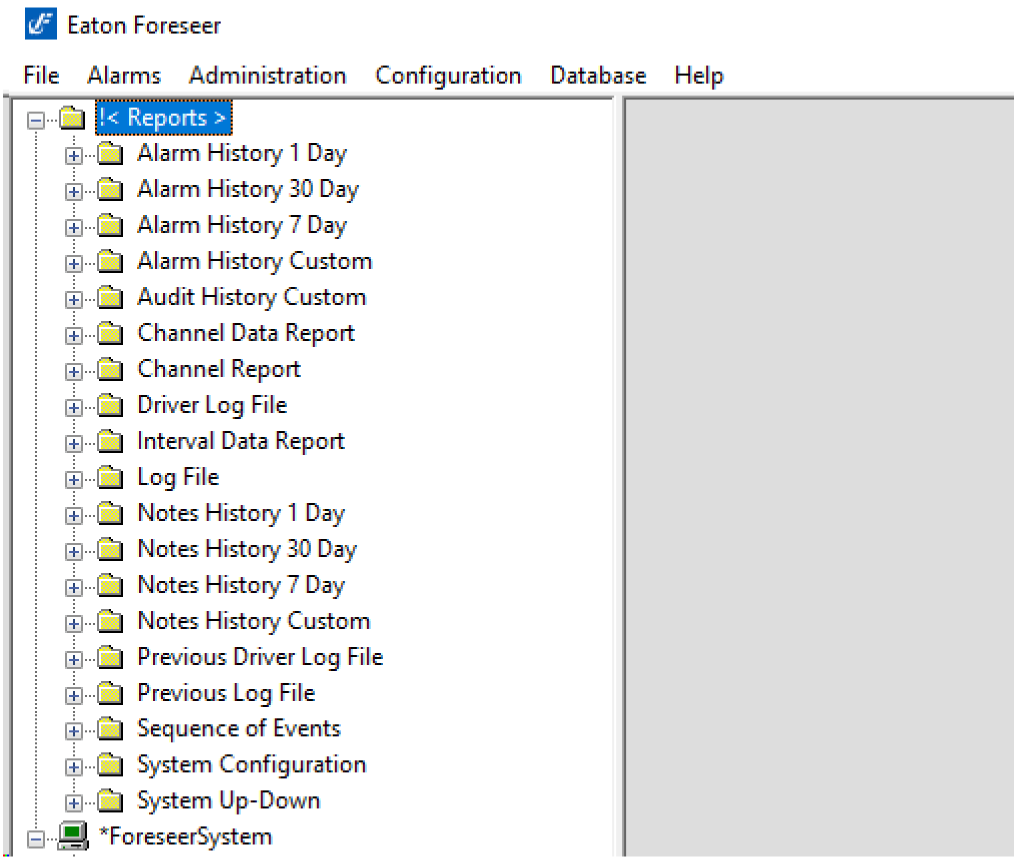
Previous Log File reports all events recorded in the previous Foreseer Server session.

System Configuration enumerates all configured Devices, their operational parameters and current interface software version.

System Up-Down reports each time the Foreseer program was launched and terminated.

Choose <Reports> in the left pane of the Tree View to access this Foreseer function. The list of **Reports** in a particular format is expanded by clicking on the "**+**" which precedes its associated folder; pressing "**-**" contracts them. The last three Reports, including the time and date they were last Run and their file size, are displayed. You can Retrieve any of these **Reports** or Run new ones. A retrieved **Report** can be viewed, printed or incorporated into other documents, if desired.

✓ A **Report** must be Run before its data can be Retrieved.



!< Reports >
- Alarm History 1 Day
- Alarm History 30 Day
- Alarm History 7 Day
- Alarm History Custom
- Audit History Custom
- Channel Data Report
- Channel Report
- Driver Log File
- Interval Data Report
- Log File
- Notes History 1 Day
- Notes History 30 Day
- Notes History 7 Day
- Notes History Custom
- Previous Driver Log File
- Previous Log File
- Sequence of Events
- System Configuration
- System Up-Down

*ForeseerSystem

- Running Reports
- Retrieving Reports
- Custom Reports

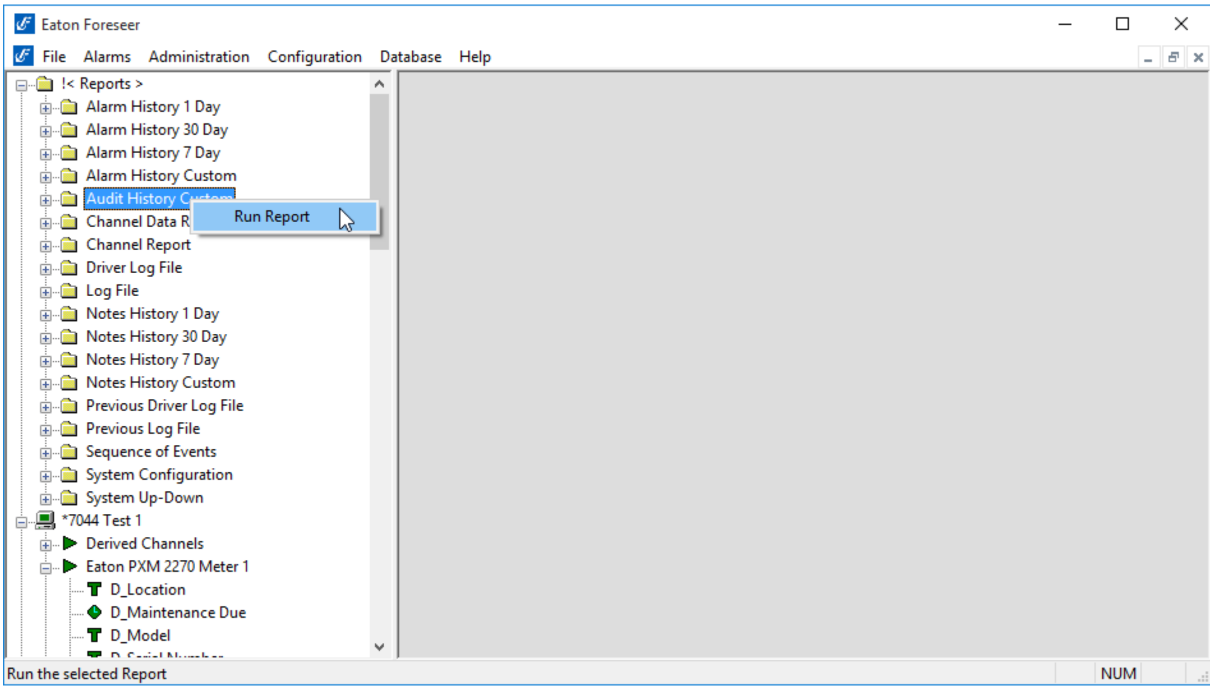
Running Reports

Running a Foreseer **Report** compiles data which is then Retrieved for display, print or incorporation into other programs.

To Run a Foreseer **Report**:

✓ Administrative Authorization is required to Run a **Report**.

1. Choose <Reports> folder in the left pane of the Tree View and click on the "**+**" preceding it to display the list of available Report Types.
2. Select the desired Report format by highlighting its folder.



3. Right-click and choose the Run Report command to compile the chosen **Report**. Display of the date, time and file size indicates that the **Report** has finished Running.
4. Open the folder, highlight the **Report** and double-click on it to display it.

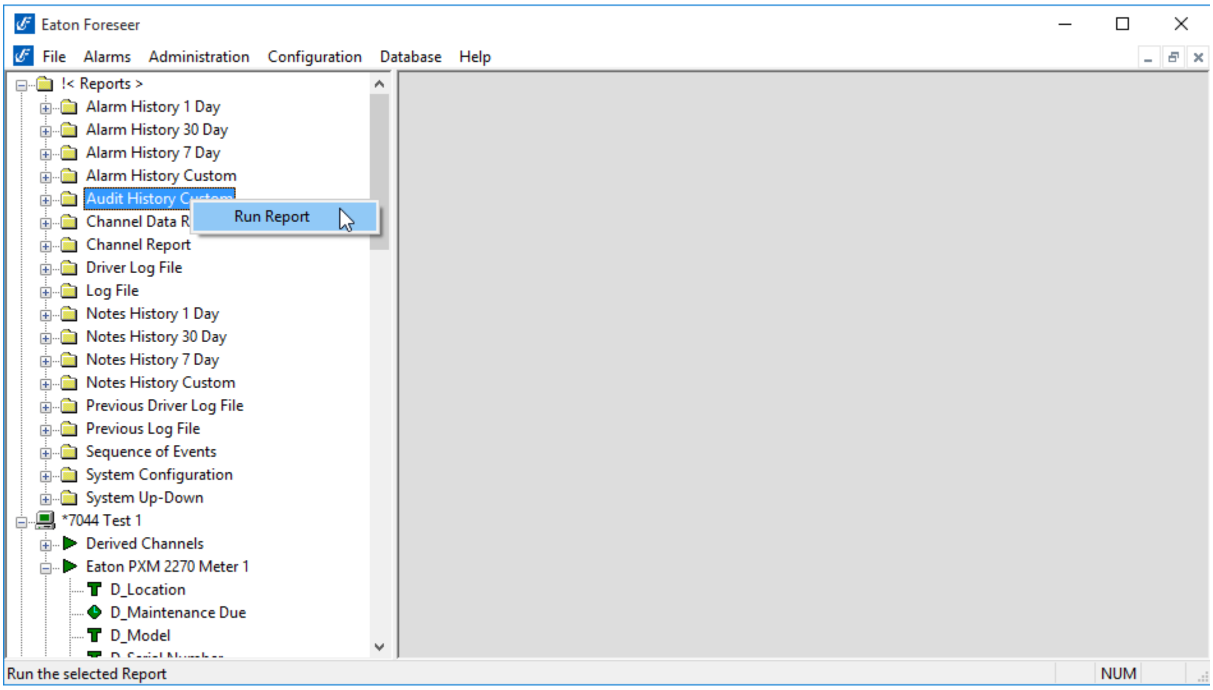
Retrieving Reports

Foreseer **Reports** that have been Run can be viewed and printed, if desired. A **Report** can also be saved as a text file imported into word processing or spreadsheet programs for further manipulation or incorporated into other documents.

To Retrieve a Foreseer **Report**:

> ✓ Administrative Authorization is required to Run a **Report**.

1. Choose <Reports> folder in the left pane of the Tree View and click on the "**+**" preceding it to display the list of available Report Types.
2. Select the desired Report folder and once again click on the "**+**" preceding it to display the last three available **Reports** of that Type.
3. Highlight the desired text file, double-click on it and the **Report** is displayed as a Notepad document where it can be saved as a text document and incorporated into other applications.



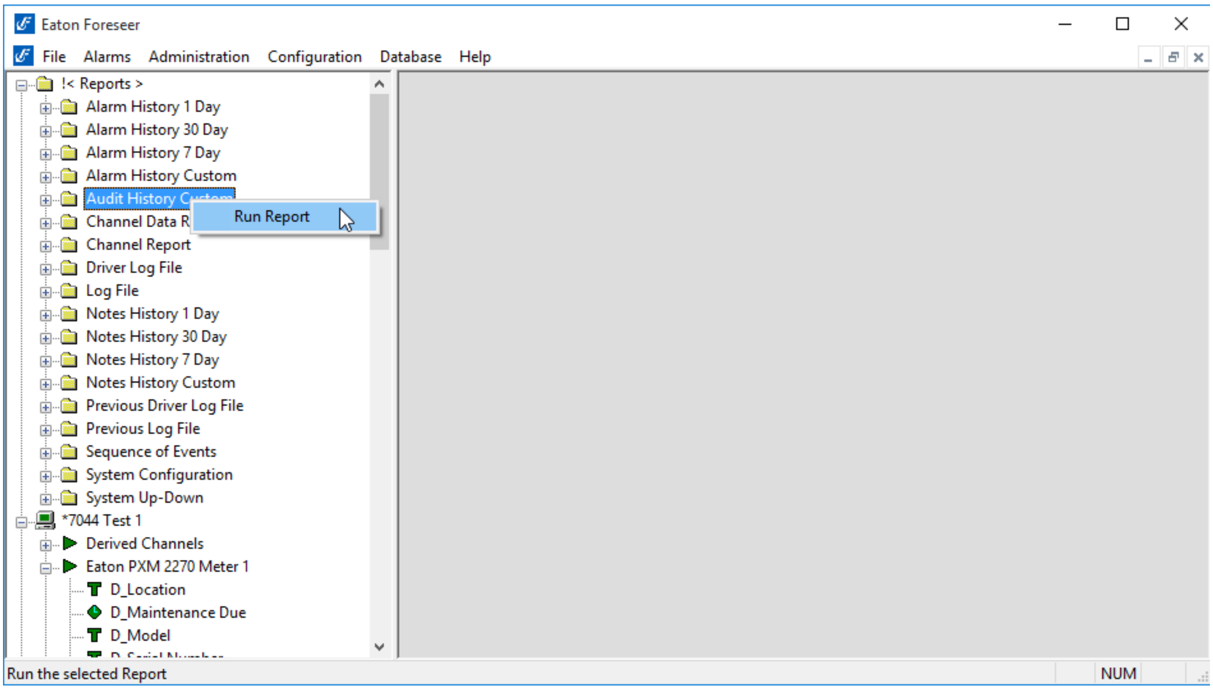
Custom Reports

Foreseer offers the ability to specify the range and content of the **Custom Alarm**, **Audit** and **Notes History Reports**. **Audit History** reports Server, Device and Channel change information. All three report formats allow you to either set a predefined interval or enter a desired period over which the report is generated. You may also choose to include or exclude certain Devices or Channels. These output selections are presented when the chosen **Custom Report** is Run.

To generate a Foreseer Custom Report:

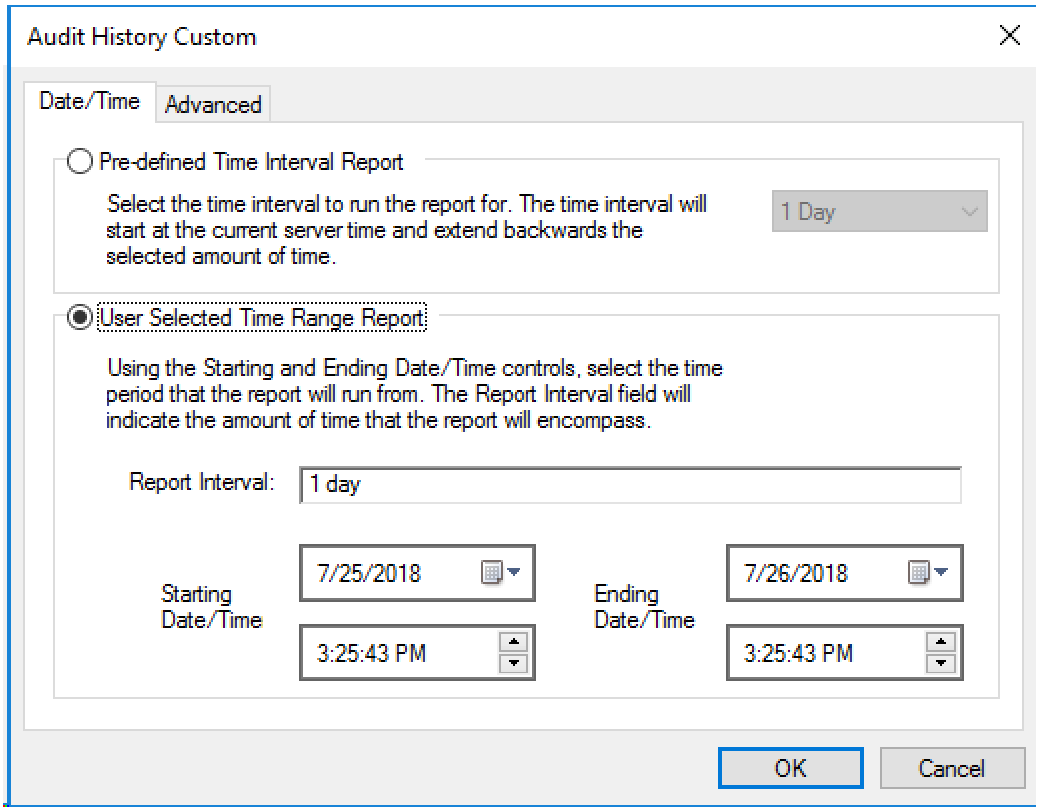
✓ Administrative Authorization is required to Run a **Report**.

1. Click on <Reports> in the left pane of the *Tree View*, followed by the "**+**" to expand the list of available Reports.
2. Select the Alarm, Audit or Notes History Custom folder.



Run the selected Report

3. Right-click and select Run Report and the appropriate **Custom History** dialog box is displayed divided into **Date/Time** and **Advanced** tabs. The tab contents, and the steps for specifying their parameters, are virtually identical for all three report formats.



○ Pre-defined Time Interval Report

Select the time interval to run the report for. The time interval will start at the current server time and extend backwards the selected amount of time.

1 Day

● User Selected Time Range Report

Using the Starting and Ending Date/Time controls, select the time period that the report will run from. The Report Interval field will indicate the amount of time that the report will encompass.

Report Interval: 1 day

Starting Date/Time: 7/25/2018 3:25:43 PM

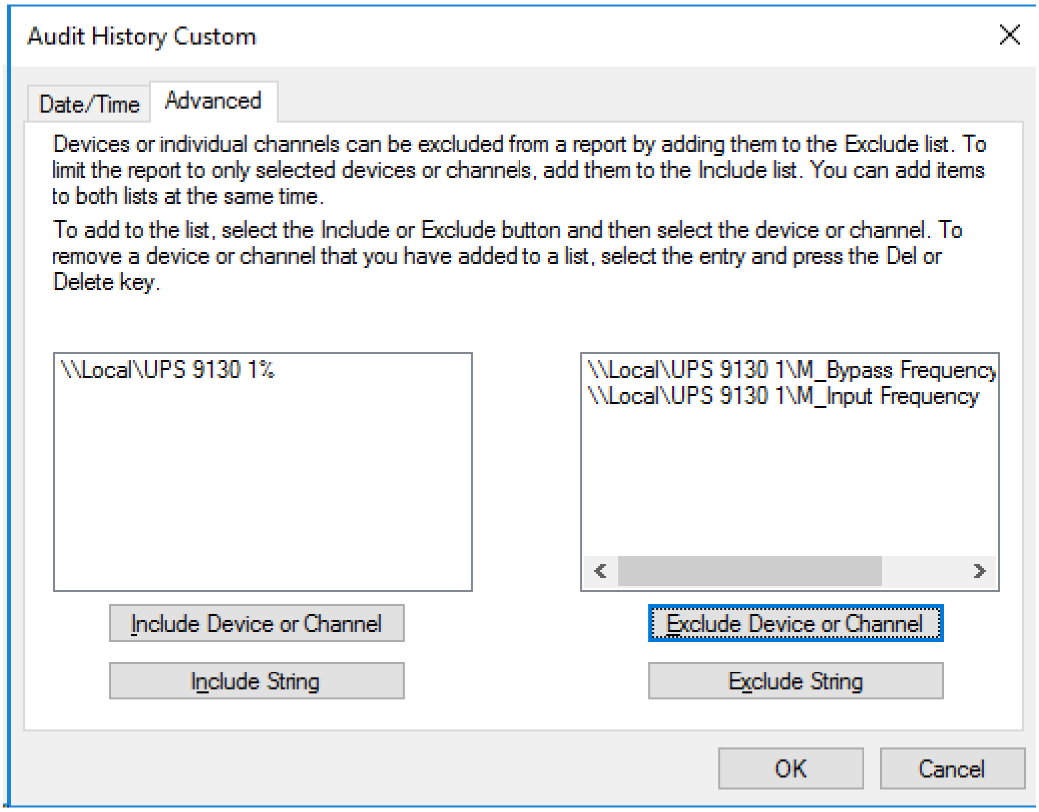
Ending Date/Time: 7/26/2018 3:25:43 PM

4. Indicate whether the **Report** will be for a Predefined Time Interval or over a Selected Time Range by clicking on the corresponding button. Choosing the former requires that you select the predefined Interval from the associated drop list. Using a Selected Time Range requires that you enter a Starting and Ending Date/Time to define the span. Any

active alarms are always reported in the Alarm History Report using the predefined Interval format, which always includes the current Server time as the Ending Time. In either case, the resulting Report Interval is calculated and shown.

✓ All active Foreseer alarms are included in the report regardless of the selected time range.

5. With the reporting period defined, click on the **Advanced** tab to display those **Custom Report** parameters.



Audit History Custom

Date/Time | Advanced

Devices or individual channels can be excluded from a report by adding them to the Exclude list. To limit the report to only selected devices or channels, add them to the Include list. You can add items to both lists at the same time.

To add to the list, select the Include or Exclude button and then select the device or channel. To remove a device or channel that you have added to a list, select the entry and press the Del or Delete key.

\\Local\UPS 9130 1%

\\Local\UPS 9130 1\M_Bypass Frequency
\\Local\UPS 9130 1\M_Input Frequency

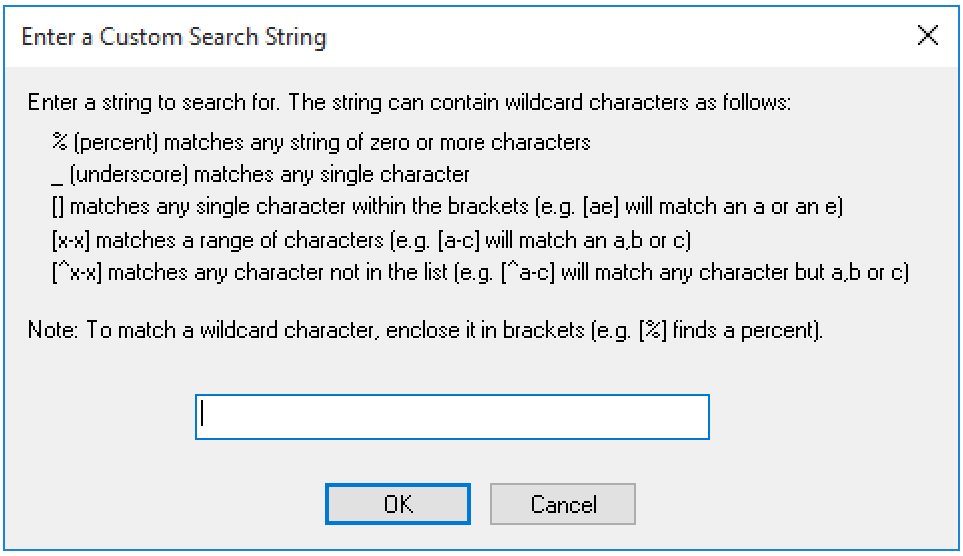
6. By default, all Devices and channels are included in a Custom History report, although you can limit the data that is reported. Click the Include or the Exclude Device or Channel button, depending on the desired information, and the Select a Device or Channel dialog box is presented.
7. Expand the list under the appropriate Server to access its connected Devices and individual channels.
8. Highlight the desired Device(s) and/or channel(s) and press OK to add them to the Include or Exclude list. Entries can be made to both lists simultaneously. To remove an entry from either list, simply select it and press the Delete key. Uncheck the Include System Up/Down Notes in Report field if you do not want this information in a Custom Notes History.
9. With the desired output criteria specified, click OK and the Custom History report is Run.
10. Open the appropriate Custom History folder, select the completed Report and press

Retrieve to display it.

Custom Search Strings

The ability to perform specific text searches on Custom History files can be extremely useful in locating archived information about a particular event or piece of equipment. To perform a custom search:

1. Click on the Include or Exclude String button in the **Advanced Custom History** dialog box as appropriate and a **Custom Search String** dialog box is displayed.

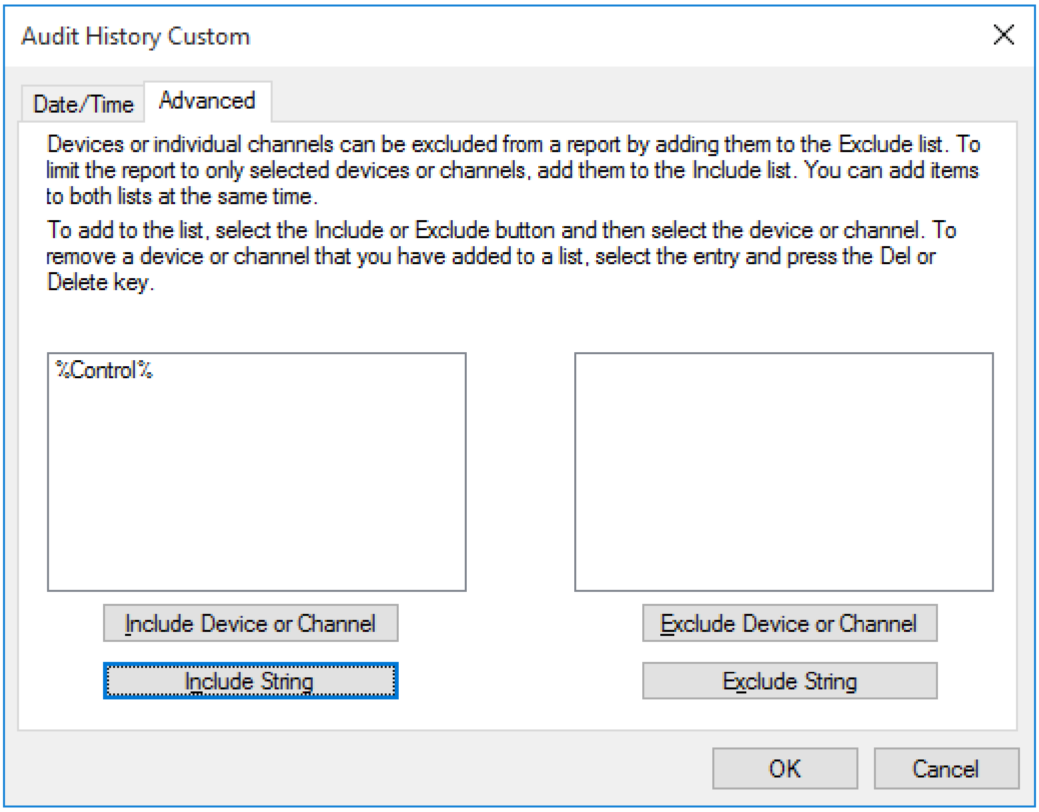


Enter a string to search for. The string can contain wildcard characters as follows:

% (percent) matches any string of zero or more characters
_ (underscore) matches any single character
[] matches any single character within the brackets (e.g. [ae] will match an a or an e)
[x-x] matches a range of characters (e.g. [a-c] will match an a,b or c)
[^x-x] matches any character not in the list (e.g. [^a-c] will match any character but a,b or c)

Note: To match a wildcard character, enclose it in brackets (e.g. [%] finds a percent).

2. Enter the text string to be included or excluded in the field provided, using wild-cards in most instances, and click OK to return to the **Advanced Custom History** dialog box. The entered string appears in the appropriate list box. You can repeat the procedure to add additional text strings to further refine your search criteria.



Devices or individual channels can be excluded from a report by adding them to the Exclude list. To limit the report to only selected devices or channels, add them to the Include list. You can add items to both lists at the same time.

To add to the list, select the Include or Exclude button and then select the device or channel. To remove a device or channel that you have added to a list, select the entry and press the Del or Delete key.

%Control%

3. With the desired text string(s) entered, click OK to perform the specified search and a file is created containing the results.
4. Select the file from the Reports Available list and click Retrieve.
5. Save the file and the search results are displayed.

System Administration

System Administration is an advanced Foreseer function which dictates various aspects of program operation. It includes the ability to:

✓ Administrative Authorization to access System Administration.

- Login , Logoff and Change the Server Password
- Change Passwords
- Start and End Database Sessions
- Start and End Server Configuration Sessions
- Backup and Check Databases
- Backup the Server Configuration
- Device Installation
- Modify Meters (analog) or Status (digital) **Channel Properties**
- Add or Delete a Device or Channel
- Add User-Defined Channels

- Configure Message Management
- Modify Server Properties

- System Properties
- LDAP Properties
- WebViews
- Server Service
- Security and User Groups
- Redundant and Remote Servers

System Properties

- File Management
- Administration Authorization
- Client Connection Password

File Management

Foreseer has made it easy to update program software modules as they are released. You can upload Device driver files. When issued, these files are installed in the Update VI folder. You can also create VI files.

To update driver files:

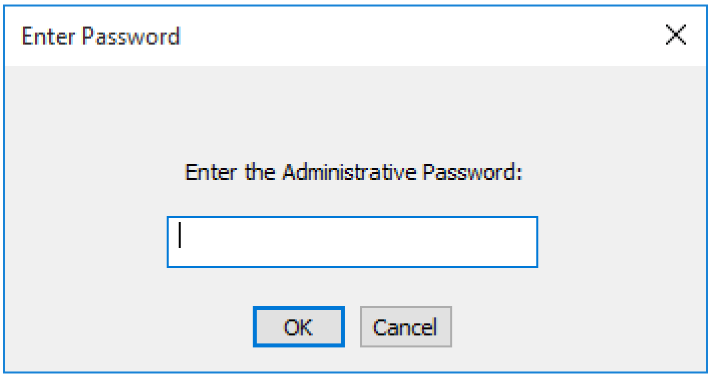
1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

   "********SERVER CONFIGURATION MODE********

   " is displayed in the Windows title bar to confirm operational status.
2. To update Device driver files, select the desired Device, and choose the Disable command from either the Configuration menu or the right-click menu.
3. Right-click and choose Unload Driver to automatically remove the outdated file.
4. Right-click again and specify Load Driver. The file is retrieved from the Update VI folder and installed automatically.
5. With the Device still selected, choose Enable from the Configuration menu or right-click menu.
6. With all file updates completed, choose End Server Configuration in the Configuration menu to restore normal Server operation.

Administrative Authorization

Password protection ensures that only authorized personnel are allowed to alter the Foreseer Server configuration or halt its data gathering and system monitoring operations. When enabled, a security password must be entered before most Server functions can be accessed. The first attempt to alter protected Server settings requires the **Administrative Password**. The password is entered in the **Administrative Password** dialog box; asterisks are displayed to maintain system security. The accepted entry automatically becomes part of the System Log and is available for review in that Foreseer Report. Once entered, the user has access privilege to all protected Server functions and does not have to enter the password again during the current session.

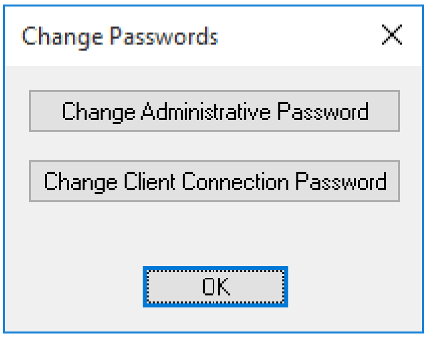

Enter Password

Enter the Administrative Password:

The Administrative and Client Connection Passwords may be changed, or assigned at a later time if one was not specified during initial Server configuration. The **Change Passwords** dialog box permits these Foreseer Server authorizations to be altered. Changing a Password does require entry of the Old password before you are allowed access the New password field.

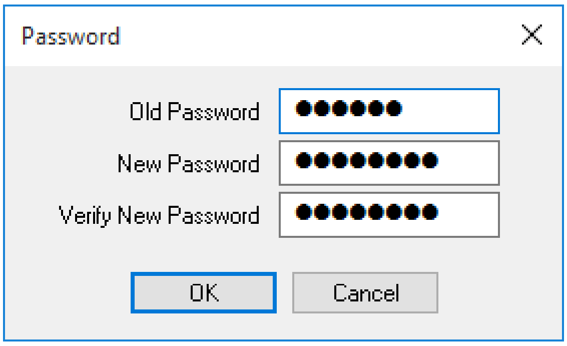
To change the Server's current Administrative password:

1. Select Change Passwords... under the Administration menu and the **Change Server Password** dialog box is displayed.


Change Passwords

Change Administrative Password
Change Client Connection Password
OK

2. Click on the Change Administrative Password or the Change Client Connection Password button to display the appropriate dialog box.



Old Password ●●●●●●

New Password ●●●●●●●●

Verify New Password ●●●●●●●●

3. Enter the Old Password; asterisks are displayed to maintain system security. If no Password was previously assigned, simply **Tab** to the New Password field.
4. Enter the desired New Password.

> Passwords are case-sensitive; therefore "USER," "User" and "user" are all recognized as different Passwords.

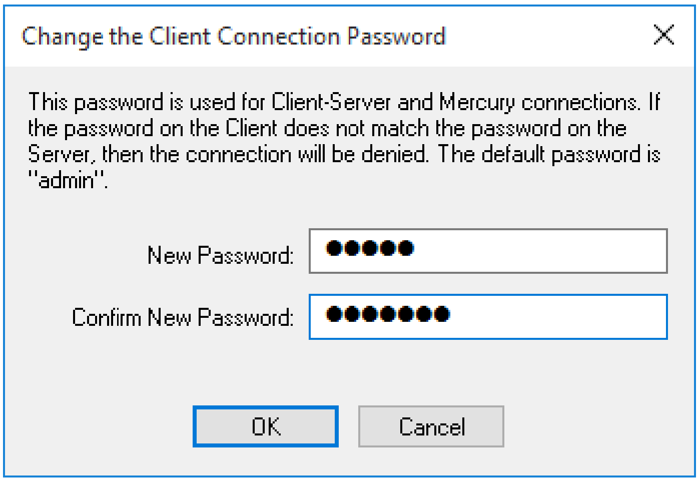
5. Type the same character string in the Verify New Password field to validate the New Password.
6. Click OK to save the New Password.

Client Connection Password

A password is used to prevent an unauthorized Foreseer Client from accessing the Server and modifying its configuration, such as changing channel properties. This Client Connection Password must agree with the Server Password entered on the Client or they will not be able to establish communications. The Connection Password may be changed by a User with Administrative Authorization privileges.

To change the Server's Client Connection Password:

1. Select Change Passwords... in the Administration menu to access the **Change Server Passwords** dialog box.
2. Click on the Change Client Connection Password button to display that dialog box.



Change the Client Connection Password

This password is used for Client-Server and Mercury connections. If the password on the Client does not match the password on the Server, then the connection will be denied. The default password is "admin".

New Password: ●●●●●

Confirm New Password: ●●●●●●●

3. Enter the New Password, then again in the Confirm field in order to verify the change. Observe the same naming conventions as those used for other Foreseer passwords, such as case sensitivity. Foreseer is shipped with "special" as the default Client Connection Password. This default allows Users with older versions of the Foreseer Client software that do not support this security feature to have access to the Server.
4. Click OK to implement the New Password. Be aware that all subscribing Foreseer Clients must know and enter the New Password locally or they no longer will be able to access the Server.

> ⓘ **Do not** specify a Client Connection Password on a network hosting Clients running a prior version of Foreseer, or they will not be able to communicate with the Foreseer Server.

LDAP Properties

You can connect Foreseer to LDAP for delegated user authentication. This allows you to use LDAP to manage access to Foreseer via membership in LDAP user groups.
Using this feature requires that you are familiar with LDAP, its query syntax, and LDIF syntax. If you aren't, you'll need help from a member of the IT staff familiar with LDAP queries.

Note: To use this feature, you must have an account that can log on to the LDAP server and that account must have a password which doesn't expire.

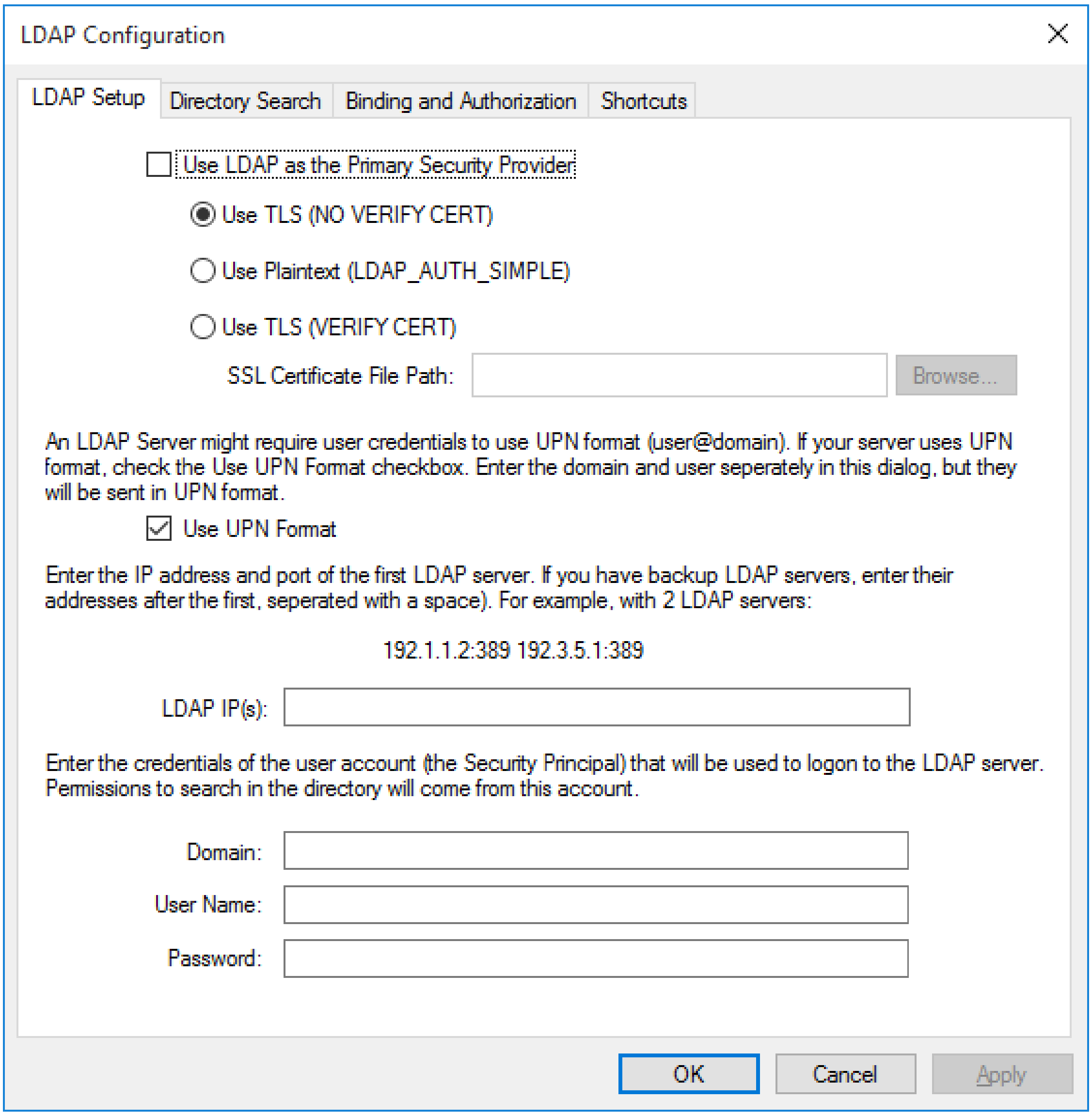
- LDAP Setup
- Directory Search
- Binding and Authorization
- Shortcuts and Branch Access

LDAP Setup

To enable LDAP authentication to Foreseer, you will need to:

- Select Use LDAP as the Primary Security Provider
- Select whether your LDAP server uses Kerberos or Plaintext to authenticate.
- Choose if your LDAP server uses user principle name for user accounts.

You must also specify the credentials for the account that is used to access the LDAP server, including the domain, user name, and user password.



□ Use LDAP as the Primary Security Provider

● Use TLS (NO VERIFY CERT)

○ Use Plaintext (LDAP_AUTH_SIMPLE)

○ Use TLS (VERIFY CERT)

SSL Certificate File Path:

An LDAP Server might require user credentials to use UPN format (user@domain). If your server uses UPN format, check the Use UPN Format checkbox. Enter the domain and user seperately in this dialog, but they will be sent in UPN format.

☑ Use UPN Format

Enter the IP address and port of the first LDAP server. If you have backup LDAP servers, enter their addresses after the first, seperated with a space). For example, with 2 LDAP servers:

192.1.1.2:389 192.3.5.1:389

LDAP IP(s):

Enter the credentials of the user account (the Security Principal) that will be used to logon to the LDAP server. Permissions to search in the directory will come from this account.

Domain:

User Name:

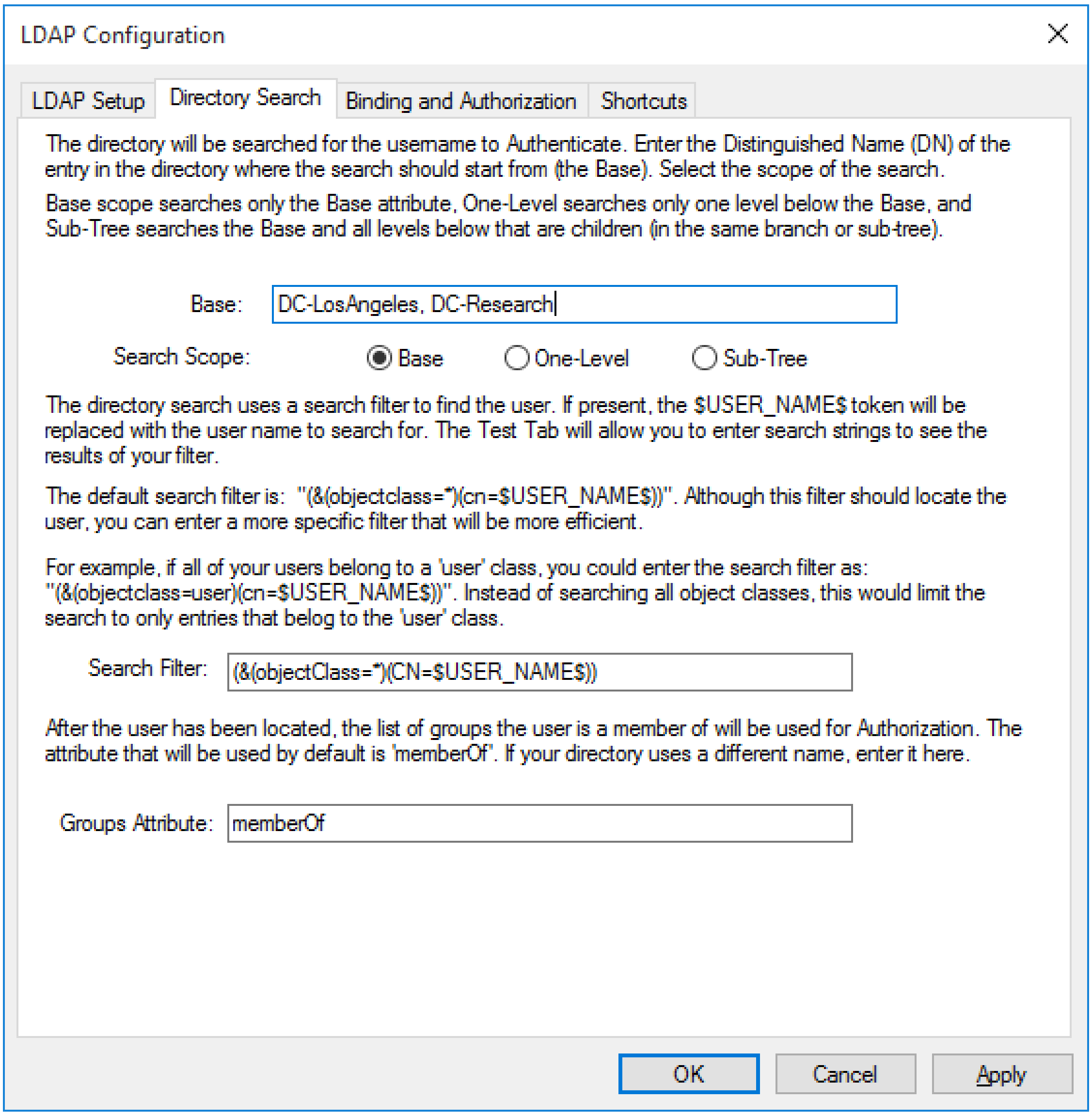
Password:

Directory Search

You must set the base distinguished name (dn) that Foreseer will use to run queries on the directory server. The subtree search starts from this distinguished name. You must also set the query depth (Search Scope).

The filter that preloaded in the Search Filter was designed to find user objects in most situations. However, you can enter your own string tailored to your system. The example shown in the following figure has such a string.

The final field specifies the attribute that will return all groups to which a user belongs. If you use a different attribute you need to replace the default string.



The directory will be searched for the username to Authenticate. Enter the Distinguished Name (DN) of the entry in the directory where the search should start from (the Base). Select the scope of the search.

Base scope searches only the Base attribute, One-Level searches only one level below the Base, and Sub-Tree searches the Base and all levels below that are children (in the same branch or sub-tree).

Base: DC-LosAngeles, DC-Research

Search Scope: ● Base ○ One-Level ○ Sub-Tree

The directory search uses a search filter to find the user. If present, the $USER_NAME$ token will be replaced with the user name to search for. The Test Tab will allow you to enter search strings to see the results of your filter.

The default search filter is: "(&(objectclass=*)(cn=$USER_NAME$))". Although this filter should locate the user, you can enter a more specific filter that will be more efficient.

For example, if all of your users belong to a 'user' class, you could enter the search filter as: "(&(objectclass=user)(cn=$USER_NAME$))". Instead of searching all object classes, this would limit the search to only entries that belog to the 'user' class.

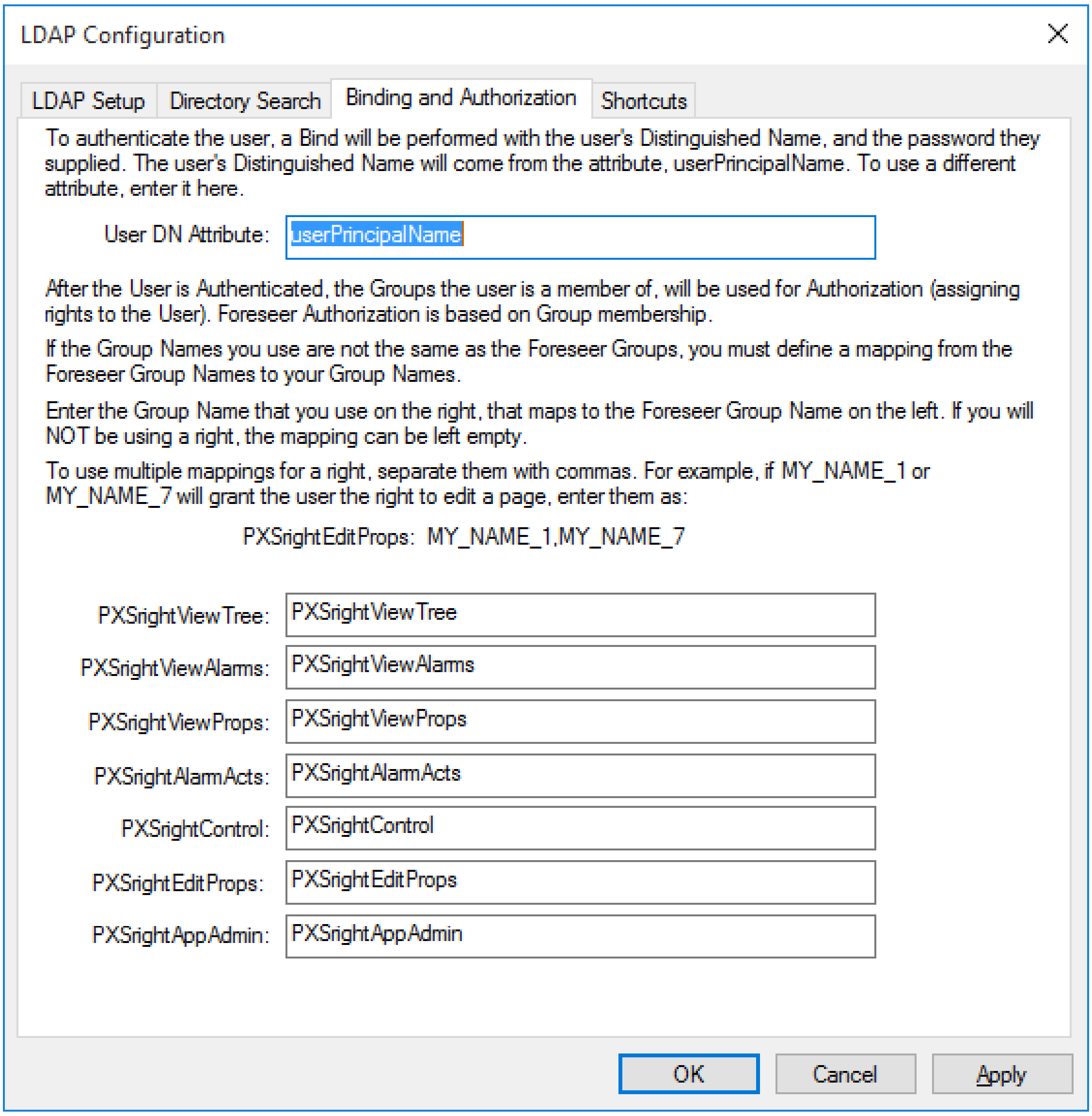
Search Filter: (&(objectClass=*)(CN=$USER_NAME$))

After the user has been located, the list of groups the user is a member of will be used for Authorization. The attribute that will be used by default is 'memberOf'. If your directory uses a different name, enter it here.

Groups Attribute: memberOf

Binding and Authorization

This tab associate's groups to which a user belongs to Foreseer groups, granting that user rights within Foreseer. Essentially, you specify the attribute that returns the distinguished name in the user DN Attribute field and then map objects that define user groups in LDAP in the appropriate Foreseer group field. Typically, you will be matching on common name (CN) objects, as is shown in the example. If you wish to grant membership in a Foreseer group to multiple LDAP user groups, separate these object definitions with a comma. For more about Foreseer groups, see the *Foreseer Server Guide*.



To authenticate the user, a Bind will be performed with the user's Distinguished Name, and the password they supplied. The user's Distinguished Name will come from the attribute, userPrincipalName. To use a different attribute, enter it here.

User DN Attribute: userPrincipalName

After the User is Authenticated, the Groups the user is a member of, will be used for Authorization (assigning rights to the User). Foreseer Authorization is based on Group membership.

If the Group Names you use are not the same as the Foreseer Groups, you must define a mapping from the Foreseer Group Names to your Group Names.

Enter the Group Name that you use on the right, that maps to the Foreseer Group Name on the left. If you will NOT be using a right, the mapping can be left empty.

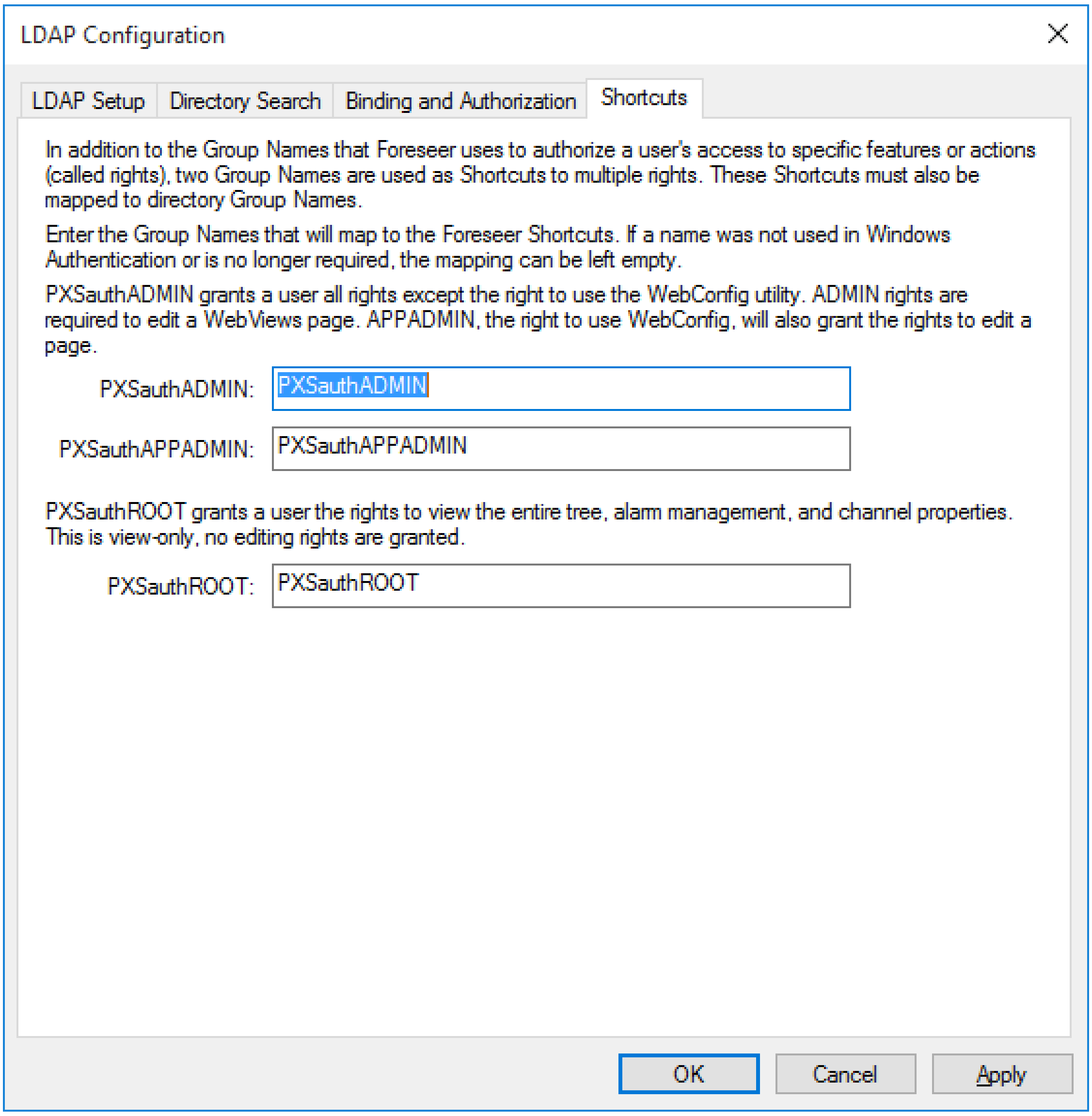
To use multiple mappings for a right, separate them with commas. For example, if MY_NAME_1 or MY_NAME_7 will grant the user the right to edit a page, enter them as:

PXSrightEditProps: MY_NAME_1,MY_NAME_7

PXSrightViewTree:	PXSrightViewTree
PXSrightViewAlarms:	PXSrightViewAlarms
PXSrightViewProps:	PXSrightViewProps
PXSrightAlarmActs:	PXSrightAlarmActs
PXSrightControl:	PXSrightControl
PXSrightEditProps:	PXSrightEditProps
PXSrightAppAdmin:	PXSrightAppAdmin

Shortcuts and Branch Access

Foreseer has two "superuser" groups: PXSauthADMIN and PXSauthROOT. You can also map these to LDAP user groups. For more about Foreseer user groups, see the *Foreseer Server Guide*.



In addition to the Group Names that Foreseer uses to authorize a user's access to specific features or actions (called rights), two Group Names are used as Shortcuts to multiple rights. These Shortcuts must also be mapped to directory Group Names.

Enter the Group Names that will map to the Foreseer Shortcuts. If a name was not used in Windows Authentication or is no longer required, the mapping can be left empty.

PXSauthADMIN grants a user all rights except the right to use the WebConfig utility. ADMIN rights are required to edit a WebViews page. APPADMIN, the right to use WebConfig, will also grant the rights to edit a page.

PXSauthADMIN: PXSauthADMIN

PXSauthAPPADMIN: PXSauthAPPADMIN

PXSauthROOT grants a user the rights to view the entire tree, alarm management, and channel properties. This is view-only, no editing rights are granted.

PXSauthROOT: PXSauthROOT

WebViews

Safeguarding the information stored in the Foreseer Server database while allowing Internet access can present problems if the data is sensitive. Increasingly, organizations are using digital Server Certificates to ensure confidential communications be- tween the Server and Client. Foreseer has implemented a Secure Sockets Layer (SSL) protocol which can be used to authenticate to both the WebViews/WebAdmin server and the Apache server. Use of the secure Foreseer HTTPS Server requires a Private Key Password and a Server Certificate.

User authentication and access control historically are based on a name/password scheme. But this approach requires management of a name/password database and provides limited security. A digital Certificate is a type of identification in the form of a data file that links an organization's identity to their ownership of a Public Key. This Public Key, embedded in the Certificate, is uniquely linked to a corresponding Private Key Password to which only the owner of the Certificate has access. The two Keys and the corresponding Certificate are used not only for user authentication and access control, but also for such security measures as message integrity. Such an approach affords a secure form of authentication on both ends of the connection.

Certificates of Authentication can be self-signed or purchased from a third-party source, depending on individual corporate policy. Third-party Certificate Authorities specialize in Certificate issuance and subsequent management. They take responsibility for ensuring that the company requesting the Certificate is the company it claims to be, as well as verifying anyone attempting to access the resident database. A utility is provided in the Server folder to facilitate obtaining third party certification.

The Foreseer HTTPS Web Server is enabled by default and is almost identically to the HTTP Web Server. The exception for the WebConfig server is an additional tab which requires the Private Key Password be entered to ensure any secure communications between the Server and Client. This is accessible through the Foreseer Server application itself under Administration > WebViews Server > HTTPS Server

- HTTP WebViews Server Properties
- HTTPS WebViews Server Properties

HTTP WebViews Server Properties

The **HTTP WebViews Server Properties** dialog box is used to configure the Foreseer Server for non-secure Web Browser access, thereby allowing Device status and data to be observed as well as furnishing limited Foreseer **Report** and **Alarm Management** functions. Simply click on the appropriate tab for the desired settings:

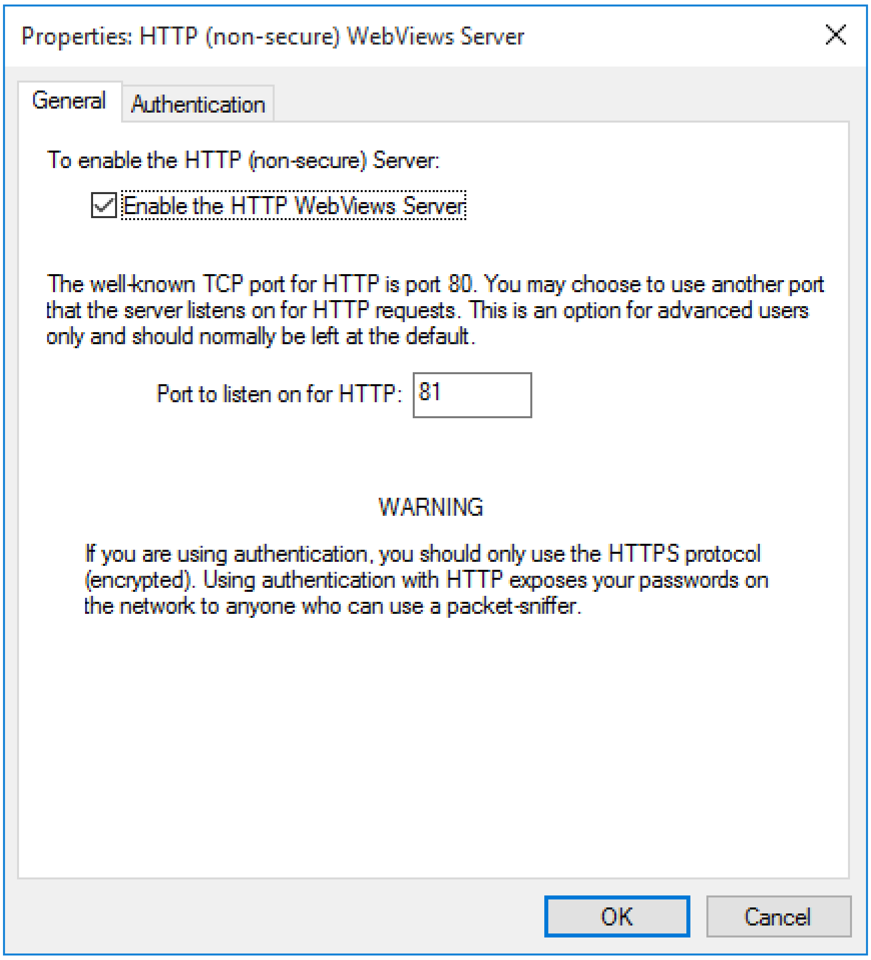
General - Allows you to Enable the HTTP (non-secure) WebViews Server, specify the Port to Listen to for HTTP connection and define the Maximum Number of Connections the Browser is permitted at one time.

Authentication - Provides a way to test the privilege (Windows user group) memberships for any Windows Account.

HTTP WebViews Server Properties - General

The **HTTP WebViews Server Properties** dialog box is used to configure the Foreseer Server for non-secure Web Browser access.

General Properties Enable HTTP Server operation, specify the Maximum Number of Connections the Browser is permitted at one time and define the Refresh Interval. Clicking in a field below displays its function: Clicking other tabs presents those **HTTP Server Properties**.



Properties: HTTP (non-secure) WebViews Server

To enable the HTTP (non-secure) Server:

☑ Enable the HTTP WebViews Server

The well-known TCP port for HTTP is port 80. You may choose to use another port that the server listens on for HTTP requests. This is an option for advanced users only and should normally be left at the default.

Port to listen on for HTTP: 81

WARNING

If you are using authentication, you should only use the HTTPS protocol (encrypted). Using authentication with HTTP exposes your passwords on the network to anyone who can use a packet-sniffer.

To view General HTTP Server Properties:

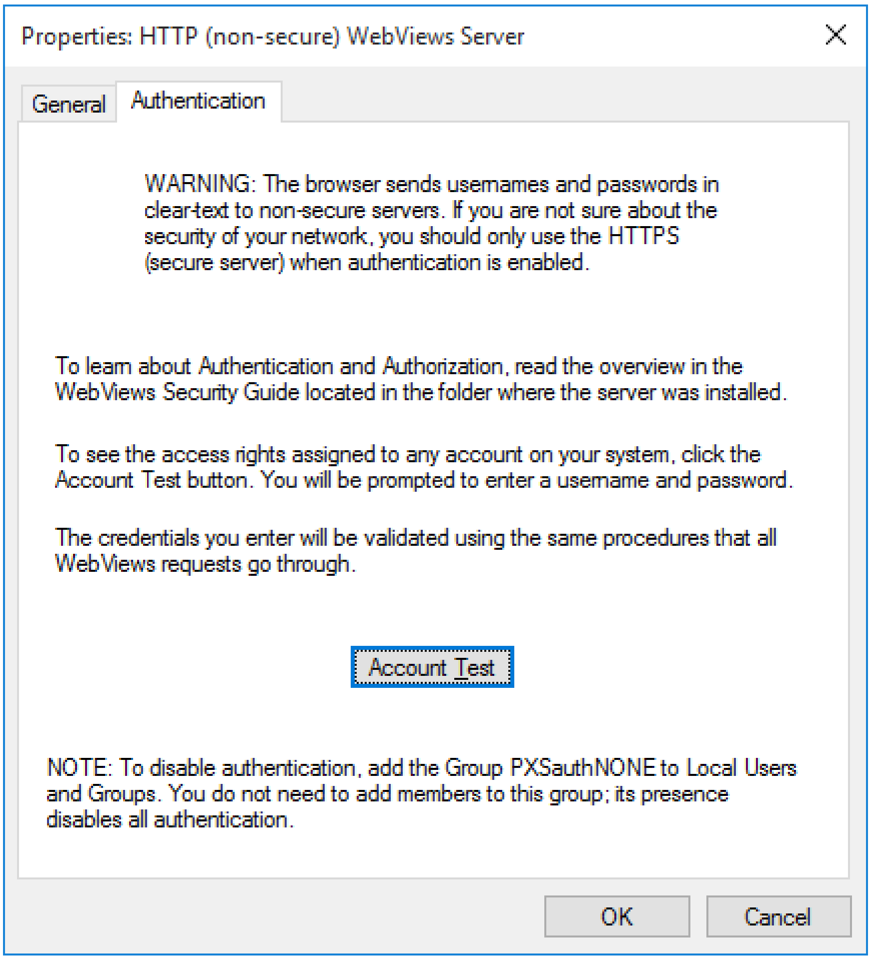
1. Select WebViews Server> HTTP Server... in the Administration menu and the **HTTP WebViews Server Properties** dialog box is displayed.
2. Click on the **General** tab to display those **HTTP Server Properties**.
3. Check the appropriate Enable the HTTP (non-secure) WebViews Server to activate this Foreseer function.

✓ You will have to restart the Server application to enable (or disable) this function.

4. If necessary, alter the Port to listen on. The default value should be adequate in most cases. If you change the port, you must also change the port number in the WebviewsFileMonitor.exe.config file in the C:\Program Files\Eaton Corporation\Eaton WebViews File Monitor folder (this is the default location).
5. With the desired settings displayed, press OK to close this dialog box or click on the other tabs to review those **HTTP WebViews Server Properties**.

HTTP WebViews Server Properties - Authentication

This tab provides a way to test the privilege (Windows user group) memberships for any Windows Account.



WARNING: The browser sends usernames and passwords in clear-text to non-secure servers. If you are not sure about the security of your network, you should only use the HTTPS (secure server) when authentication is enabled.

To learn about Authentication and Authorization, read the overview in the WebViews Security Guide located in the folder where the server was installed.

To see the access rights assigned to any account on your system, click the Account Test button. You will be prompted to enter a username and password.

The credentials you enter will be validated using the same procedures that all WebViews requests go through.

NOTE: To disable authentication, add the Group PXSauthNONE to Local Users and Groups. You do not need to add members to this group; its presence disables all authentication.

Click the Account Test button and enter the account information to test privileges.

HTTPS WebViews Server Properties

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for secure Web Browser access, thereby allowing Device status and data to be observed as well as furnishing limited Foreseer **Report** and **Alarm Management** functions. Simply click on the appropriate tab for the desired settings:

General - Allows you to Enable the HTTPS (secure) WebViews Server, specify the Port to Listen to for HTTPS connection and define the Maximum Number of Connections the Browser is permitted at one time.

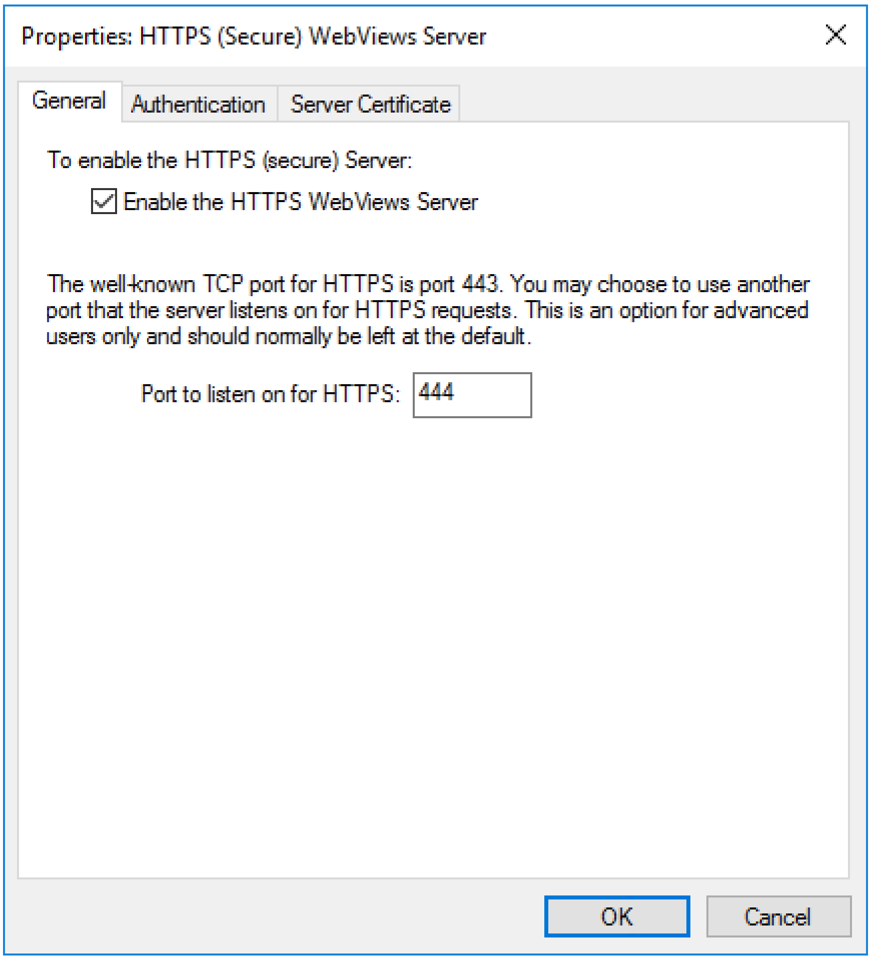
Authentication - Provides a way to test the privilege (Windows user group) memberships for any Windows Account.

Server Certificate - Allows a secure connection to be established between the Foreseer

Client and the WebViews Server.

HTTPS WebViews Server Properties - General

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for secure Web Browser access. **General Properties** Enable HTTPS Server operation, specify the Maximum Number of Connections the Browser is permitted at one time and define the Refresh Interval. Clicking in a field below displays its function: Clicking other tabs presents those **HTTPS Server Properties**.



To enable the HTTPS (secure) Server:

☑ Enable the HTTPS WebViews Server

The well-known TCP port for HTTPS is port 443. You may choose to use another port that the server listens on for HTTPS requests. This is an option for advanced users only and should normally be left at the default.

Port to listen on for HTTPS: 444

Foreseer HTTPS WebViews Server Properties settings are easily established to permit Web Browser access.

To view **General HTTPS Server Properties**:

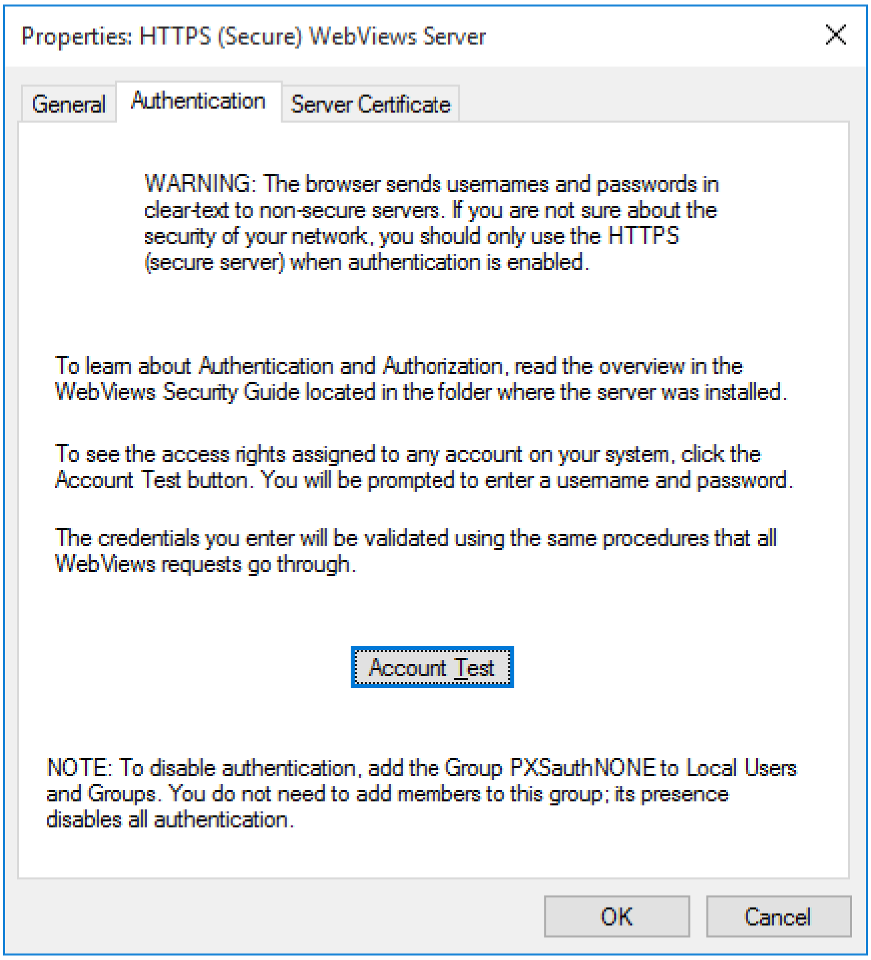
1. Select WebViews Server> HTTPS Server... in the Administration menu and the **HTTPS WebViews Server Properties** dialog box is displayed.
2. Click on the **General** tab to display those **HTTPS WebViews Server Properties**.
3. Check the appropriate Enable the HTTPS (secure) WebViews Server to activate this Foreseer function.

✓ You will have to restart the Server application to enable (or disable) this function.

4. If necessary, alter the Port to listen on. The default value should be adequate for these settings in most cases. If you change the port, you must also change the port number in the WebviewsFileMonitor.exe.config file in the C:\Program Files\Eaton Corporation\Eaton WebViews File Monitor folder (this is the default location).
5. With the desired settings displayed, press OK to close this dialog box or click on the other tabs to review those **HTTPS WebViews Server Properties**.

HTTPS WebViews Server Properties - Authentication

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for Web Browser access. **Authentication Properties** furnishes a level of security by requiring Passwords to view HTTPS Server information as well as request **Reports** and Acknowledge alarms. Clicking in a field below displays its function: Clicking other tabs presents those **HTPPS Server Properties**.



WARNING: The browser sends usernames and passwords in clear-text to non-secure servers. If you are not sure about the security of your network, you should only use the HTTPS (secure server) when authentication is enabled.

To learn about Authentication and Authorization, read the overview in the WebViews Security Guide located in the folder where the server was installed.

To see the access rights assigned to any account on your system, click the Account Test button. You will be prompted to enter a username and password.

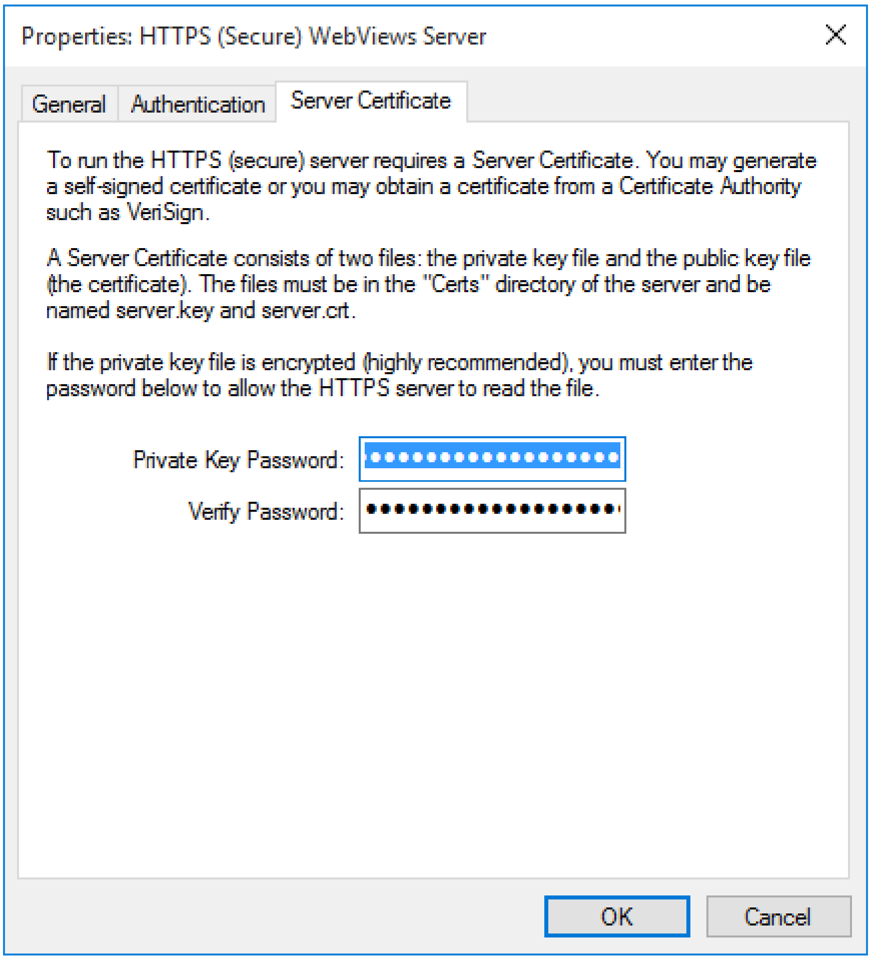
The credentials you enter will be validated using the same procedures that all WebViews requests go through.

NOTE: To disable authentication, add the Group PXSauthNONE to Local Users and Groups. You do not need to add members to this group; its presence disables all authentication.

Click the Account Test button and enter the account information to test privileges.

HTTPS WebViews Server Properties - Server Certificate

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for Web Browser access. **Server Certificate Properties** ensure only authorized Users can access the Server through a Web Browser. Clicking in a field below displays its function: Clicking other tabs presents those **HTTPS Server Properties**.



To run the HTTPS (secure) server requires a Server Certificate. You may generate a self-signed certificate or you may obtain a certificate from a Certificate Authority such as VeriSign.

A Server Certificate consists of two files: the private key file and the public key file (the certificate). The files must be in the "Certs" directory of the server and be named server.key and server.crt.

If the private key file is encrypted (highly recommended), you must enter the password below to allow the HTTPS server to read the file.

Private Key Password: ••••••••••••••••••

Verify Password: ••••••••••••••••••

Foreseer HTTPS WebViews Server Properties settings are easily established to permit Web Browser access. In this example, the necessary security files are generated through the utility supplied with Foreseer, openssl.exe.

To set **HTTPS WebViews Server Certificate Properties** :

1. In Windows Explorer, locate the file in the Foreseer **Server** folder and double-click on it. The DOS screen displays the prompt:

   OpenSSL>

2. To generate a Private Key Password, type and enter:

   genrsa -des3 -out server.key 1024

3. You are prompted for a pass phrase that will be used as the Private Key Password. It is recommended your entry be at least eight characters and include numbers and letters.

> Record the Password and store it in a secure location. You will not be able to use your Private Key or Server Certificate without it and, once entered, it cannot be recovered.

4. To generate a Certificate Signing Request at the OpenSSL> prompt, type and enter:

```
req -new -key server.key -out server.csr
```

5. Enter your Private Key Password once again at the pass phrase prompt. You will be requested to enter information which will become part of your Server Certificate identification. This information will be verified by the Certificate Authority.
6. Enter your Country Name as a 2-letter code.
7. Enter your complete State or Province Name. Do not use abbreviations
8. Enter your Locality Name, typically the city in which your company resides.
9. Enter your Organization Name. This entry must be your official company name as it appears on the Articles of Incorporation.
10. Optionally enter your Organizational Unit Name to identify your department within your company.
11. Enter your Common Name. This entry is extremely important. It is the URL for the HTTPS Server that is entered in the Web Browser and it **must be correct,** or Foreseer Users will be warned that they are cannot access the HTTPS Server. This entry can be an IP Address.
12. Enter the Email Address of the System Administrator.
13. Optionally enter a Challenge Password and the screen returns to the OpenSSL> prompt.
14. If desired, you can generate a temporary (30-day) Self-Signed Certificate by entering the following:

```
req -x509 -key server.key -in server.csr -out server.crt
```

15. Enter your Private Key Password as requested, and the Self-Signed Certificate is created.
16. Type quit to exit the Open SSL utility.
17. Locate the server.key and server.crt files in the **Server** folder and copy the server.key file into the Server **certs** folder. A server.csr which is also generated should be submitted to Verisign with your certification application.
18. In the Foreseer Server application, select HTTPS Server... in the Administration menu to display its **General Properties**.
19. Check the Enable the HTTPS (secure) Server setting to activate this function.
20. Change the Port to listen on, the Maximum Number of Connections and the Refresh Interval, if required.
21. Change the **Authentication** and **Connection Keep-Alive** settings if necessary. The

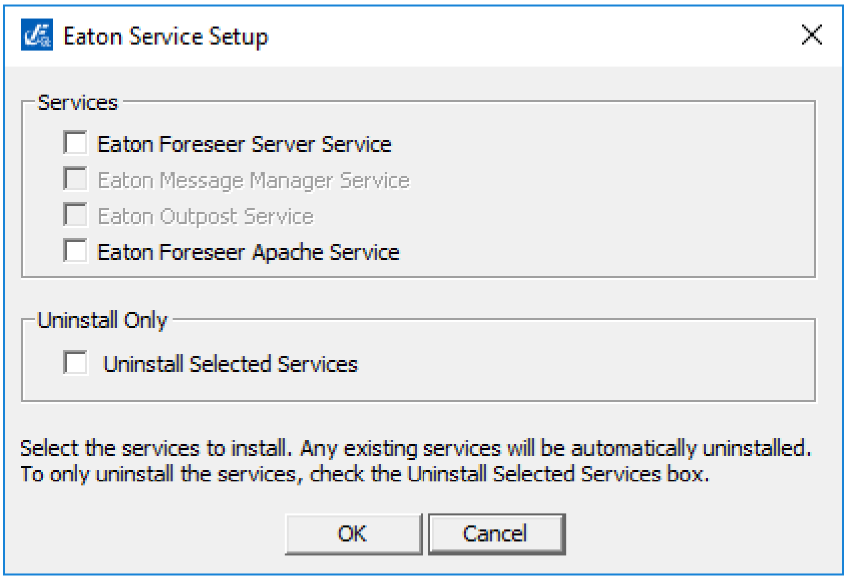
default settings should be adequate in most cases.

22. Click on the **Server Certificate** tab.
23. Enter your encrypted Private Key Password (pass phrase), then enter the Password a second time to Verify it.
24. Click OK then reboot the Server to enable the new HTTPS settings.

Any Client wishing to view the HTTPS WebViews Server will have to enter the correct Private Key Password or access is denied. A secure connection is indicated by padlock in the Browser status bar.

Server Service

The Foreseer Server must run as a Service within the Windows operating system under the local system (User Name and Password) account. In rare installation instances, the Server initially may have to be defined as a Service, or it may be desirable to uninstall it as a Service for other reasons. The **Server Service Setup** dialog box allows installation and removal of the Server as a service. Simply locate the ServiceSetup.exe file in the Foreseer **Server** program folder and double-click on it to display that dialog box. Select Install or Uninstall and click OK to execute the desired function.


Eaton Service Setup

Services

□ Eaton Foreseer Server Service
□ Eaton Message Manager Service
□ Eaton Outpost Service
□ Eaton Foreseer Apache Service

Uninstall Only

□ Uninstall Selected Services

Select the services to install. Any existing services will be automatically uninstalled.
To only uninstall the services, check the Uninstall Selected Services box.

- Server Properties

Server Properties

The **Server Properties** dialog box identifies important Foreseer Server settings and allows several administrative functions to be performed. Simply click on the appropriate tab for the desired settings:

✓ Administrative Authorization is required to access **Server Properties**.

General - Identifies the Server and configures Server startup.
Remote - Allows Server restart and software upgrade operations to be performed remotely.
Database - Determines historic database settings.
Redundant - Identifies the Server as a backup to endure continued site monitoring in the event the principle Server fails.

Security and User Groups

WebViews allows a user to view installed devices on the Foreseer Server and the system status using a standard web browser (see the Release Notes for supported versions). A users visual access level and rights can be closely controlled through WebViews authentication and authorization. Viewing access can be granted to the entire system or to the granularity of viewing a single page. Control of the system can be broad-based or locked down entirely.

- Authorization Levels
- Accounts
- User Group Privilege Details
- Updating User Groups
- Whitelisting

Authorization Levels

The authorization level granted to a user will depend on the authorization options that are in effect for the HTTP and HTTPS servers and the credentials the user presents to the server. Under no circumstances will the WebViews HTTP(S) server allow access to any file or folder above the root of the WebViews folder.

Authentication requires that a user provides both a Username and Password (their credentials). The users credentials are passed to the Windows default security provider for validation. The credentials must represent a valid Windows user account and depending on the Security Policies at your site, the account may need the Log on locally permission on the computer where the server is running. After the credentials have been validated, the server then checks to see what Groups the user is a member of.

The WebViews server currently provides three classes of authorization: ADMIN, ROOT and TOP (or Branch). The ADMIN authorization class grants the user all rights. ROOT authorization grants an account the right to View the Tree and View Alarms. TOP (Branch) authorization grants a user the ability to view a specific branch of the tree.

A TOP level folder is defined as a folder that is a direct child of /WebViews (the root folder). When an account has TOP authorization, they have access to the TOP (branch) folder and all channels and folders under (or descendants of) the branch folder. If an account has membership in both the TOP group and the ROOT group, the user will be granted the higher-level ROOT authorization (or rights).

ADMIN authorization is requested by using the root path of /WebAdmin/ instead of /WebViews/. An account that is a member of the ADMIN group (PXSauthAPPADMIN) will be granted all rights.

When a user has been authorized at the Branch level, they may not view or access any data or pages outside of the branch they have been authorized for.

The WebViews server will cache the last credentials that were presented and the rights associated with the credentials. As long as the Internet Explorer session persists, WebViews will check the credentials presented by the browser with the current request against the cached credentials. If they match, the WebViews server can skip the time-consuming step of further Authentication and Authorization.

When a new session is started or the cached rights are not sufficient for the current request, WebViews will reply to the request with an HTTP 401 status code. A 401 status is known as an Authorization Challenge. When the browser receives a challenge, it will present the user with a Login dialog. The user has three tries (the three-strike rule) to provide credentials that the server will accept. If the user cannot provide valid credentials, the browser typically displays a blank page. The WebViews server uses

HTTP Basic Authentication. The browser encodes the credentials supplied by a user and sends it to the WebViews server in the HTTP Authorization header field.

Caution: As the credentials are only encoded (not encrypted), they are subject to being intercepted and decoded. To keep credentials secure it is highly recommended that the site uses the HTTPS (secure) server when authorization is enabled. The HTTPS server uses 256-bit encryption which guarantees that even if the information that is sent is intercepted, it cannot be decoded.

A WebViews folder tree can be graphically represented as such:

WEBVIEWS			/webviews
	BASEMENT		/webviews/basement
		UPS 1	/webviews/basement/ups 1
		ATS 1	/webviews/basement/ats 1
	FLOOR 1		webviews/floor 1
		GEN A	webviews/floor 1/gen a
		GEN B	webviews/floor 1/gen b

	FLOOR 2		webviews/floor 2
		AC 1	webviews/floor 2/ac 1
		AC 2	webviews/floor 2/ac 2
		AC North	webviews/floor 2/ac north

WEBVIEWS is at the *Root* level. BASEMENT, FLOOR 1, and FLOOR 2 are the *Top* level. The devices would be at the *Branch* level.

A *TOP* level folder is a direct child of the root folder (WebViews in the example tree). *TOP* folders define a branch which includes the *TOP* folder and all folders that are descendants of the *TOP* folder. Basement, Floor 1, and Floor 2 are all *TOP* folders. The Floor 1 branch includes the following folders: /WebViews/Floor 1, /WebViews/ Floor 1/Gen A and /WebViews/Floor 1/Gen B.

Accounts

Accounts are managed by Windows and may be Local Users or Domain accounts. To allow a specific right, create a Local Group (local to the computer where the Foreseer Server is installed and running) from the following Foreseer Group Names:

User/Security Group	Details
PXSauthNONE	• Disables all authentication requirements, including access to the Web Configuration utility. • A user login will not be required to view pages, edit pages, acknowledge/ rearm alarms, change channel properties, etc. • Grants administrator permission to everyone. **This group should be used with extreme care. It grants full access to everyone that can connect to Foreseer.**
PXSauthADMIN	• No access to Web Configuration utility. • Members have all rights in WebViews. • Members can edit (WebAdmin URL) if licensed.
PXSauthAPPADMIN	• Members can access the Web Configuration Utility and also gain all rights to WebViews and WebAdmin
PXSauthROOT	• View all branches with view alarm permission. • Members can view all WebViews pages (full

	access to the WebViews tree). ● Members can view Alarms, Reports, and Channel Properties.
PXSrightViewTree	● View all branches of the tree.
PXSrightViewAlarms	● Members can view the Alarm Management page but cannot acknowledge/rearm alarms. ● Members can view all WebViews pages. ● Grants permission to view active alarms.
PXSrightViewProps	● Grants permission to view channel properties. ● Members can view all WebViews pages.
PXSrightAlarmActs	● Grants permission for alarm management (ack/rearm). ● Members can acknowledge/rearm alarms from Alarm Management. ● Members can view all WebViews pages (full access to the WebViews tree).
PXSrightControl	● Grants permission to access a channel's control ability. ● Members can access dialogs to change Setpoint, Tri-State, and Two-State Control channels and activate Switch LED or Switch Rocker Controls.
PXSrightEditProps	● Grants permission to edit channel properties. ● Members can view Channel Properties. ● Members can view all WebViews pages.
PXSrightAppAdmin	● Members can access the Web Configuration Utility and gain all rights to WebViews and WebAdmin.

Some of the rights also imply others as follows:

- PXSrightViewAlarms....................PXSrightViewTree
- PXSrightAlarmActs.......................PXSrightViewAlarms, PXSrightViewTree
- PXSrightEditProps ....PXSrightViewProps,PXSrightViewTree
- PXSrightViewProps......................PXSrightViewTree

> You can test each account if you wish through the Authentication tab on either the HTTP or HTTPS server dialog box. Click the Account Test button and then enter the User name and Password for a Windows User. If you wish, you can also specify a branch of the WebViews tree to test for access privileges.

User Group Privilege Details

Access User group	Foreseer WebConfig	WebAdmin	WebViews	View- Alarm management	Edit(Ack/rearm) Alarm management	View-Channel Properties	Edit Channel's Properties	View Active Alarms	Channel's Control ability	View all Branches of WebViews pages
PXSauthNONE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PXSauthADMIN	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PXSauthROOT	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
PXSrightViewTree	No	No	Yes	No	No	No	No	No	No	Yes
PXSrightViewAlarms	No	No	Yes	Yes	No	No	No	Yes	No	Yes
PXSrightViewProps	No	No	Yes	No	No	Yes	No	No	No	Yes
PXSrightAlarmActs	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes
PXSrightControl	No	No	No	No	No	No	No	No	Yes *6	No
PXSrightEditProps	No	No	Yes	No	No	Yes	Yes	No	No	Yes
PXSauthAPPADMIN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PXSbranch+folder	No	No	No	No	No	No	No	No	No	No

Access User group	View Branches of WebViews at and below the folder	Edit all Branches of WebViews pages	View reports	Graphs	Data Analysis(From Graph)	Data Analysis Add Channels(from Graph)
PXSauthNONE	N/A	Yes	Yes	Yes	Yes	Yes
PXSauthADMIN	N/A	Yes	Yes	Yes	Yes	Yes
PXSauthROOT	N/A	No	Yes	Yes	Yes	Yes
PXSrightViewTree	N/A	No	Yes*1	Yes	Yes	Yes
PXSrightViewAlarms	N/A	No	Yes*2	Yes	Yes	Yes
PXSrightViewProps	N/A	No	Yes*3	Yes	Yes	Yes

PXSrightAlarmActs	N/A	No	Yes*4	Yes	Yes	Yes
PXSrightControl	N/A	No	No	No	No	No
PXSrightEditProps	N/A	No	Yes*5	Yes	Yes	Yes
PXSauthAPPADMIN	N/A	Yes	Yes	Yes	Yes	Yes
PXSbranch+folder	Yes	No	No	No	No	No

Indicators	
No	Unable to access
Yes	Able to access
Yes*1	Requires another right to be able to access reports. To view reports, User needs to have the combination of PXSrightViewTree +PXSrightViewAlarms+PXSrightViewProps
Yes*2	Requires another right to be able to access reports. To view reports, User needs to have the combination of PXSrightViewAlarms +PXSrightViewProps
Yes*3	Requires another right to be able to access reports. To view reports, User needs to have the combination of PXSrightViewProps + PXSrightViewAlarms
Yes*4	Requires another right to be able to access reports. To view reports, User needs to have the combination of PXSrightAlarmActs +PXSrightViewProps
Yes*5	Requires another right to be able to access reports. To view reports, User needs to have the combination of PXSrightEditProps + PXSrightViewAlarms
Yes*6	Requires another right to be able to get to the control. Channel's Control ability (User will likely need to be mapped to an extra role in order to test out the ability).
	To get the channel control ability, user needs to have the combination of **PXSauthROOT + PXSrightControl**

Updating User Groups

Foreseer queries the list of users and groups at startup, therefore if you make a change to either the list of users or to groups this won't be read until the next time the WebViews Server starts. To force a query of the list of users and groups, you can do one of two things:

- Restart the Foreseer Server itself.
- In the Foreseer Server, select the WebViews server through Administration > WebViews Server. In the General tab, click the OK button. This restarts the Web- views server.

Whitelisting

You can further enhance security by creating a “white list” that specifies the only IP addresses or hostnames that can be used to connect to either the WebConfig Server or the WebViews/WebAdmin server. In the Foreseer Server application, you can access the WebConfig white list through Administration > Trusted Web Clients.

Once enabled, only the IP addresses or hostnames listed in the Trusted Web Clients list can access the WebConfig utility.

To create a white list for the WebViews/WebAdmin server (the Apache server), you'll need to edit the httpd.conf file in the C:\Eaton Corporation\Foreseer\Apache24\conf\
folder.

You'll be using Require directives, as shown in the following example.

```
#Turn off general access
Require all denied

# Allow a request from the following IP address Require ip
123.123.123.123

# Allows a request from the following hostname Require host
thisismyhostname

# Require all granted
```

The "Require all granted" line must be commented to prevent everyone from having access. For more information about creating whitelists and blacklists for Apache, see:

http://httpd.apache.org/docs/current/howto/access.html.

Redundant and Remote Servers

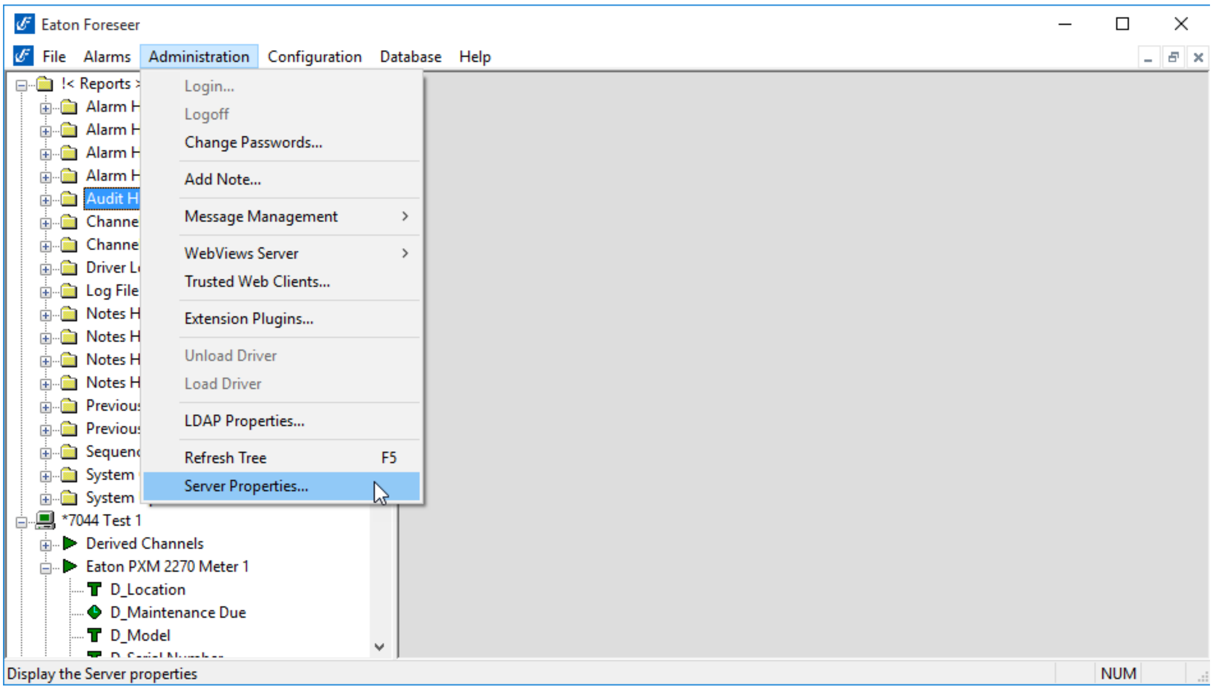
When you synchronize a Redundant Server from a Primary Server, a partial configuration backup is transferred to the redundant server. This backup contains all device configuration parameters and includes WebViews as well. It does not change items such as the Database connection settings. Note that the Redundant Server will perform a restart in order to restore and implement the updates from the primary server. Also note that both server names must be identical.

- Primary Server Setup
- Setting up a Redundant Server
- Adding The Redundant Server As A Remote On The Primary Server
- Synchronizing the Redundant Server
- Add Remote Server

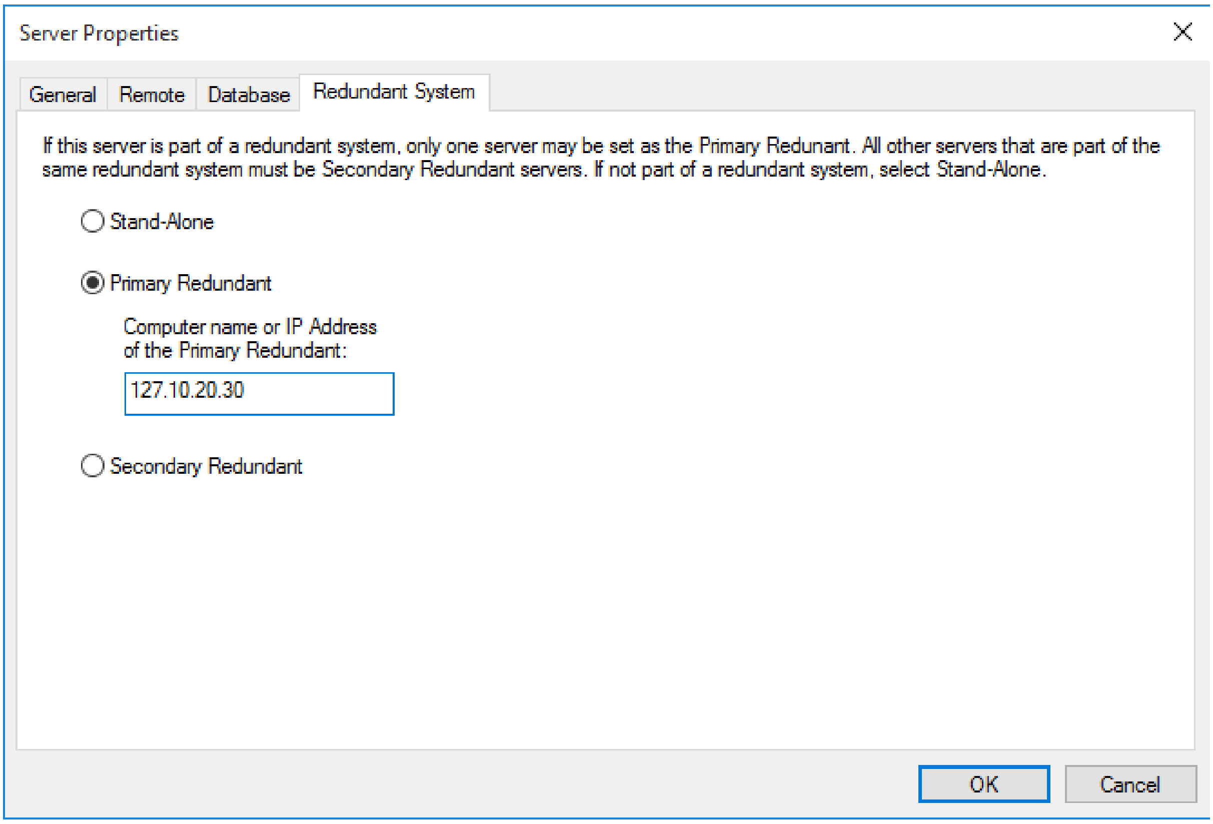
Primary Server Setup

On the Primary Server, perform the following steps with Foreseer running as an application:

1. On the Primary Server, select Administration>Server Properties.



2. Navigate to the ‘Redundant System’ tab and select the ‘Primary Redundant’ set- ting. Fill in the computer name or IP address of the Primary Redundant system. Click OK.



If this server is part of a redundant system, only one server may be set as the Primary Redunant. All other servers that are part of the same redundant system must be Secondary Redundant servers. If not part of a redundant system, select Stand-Alone.

○ Stand-Alone

● Primary Redundant

Computer name or IP Address of the Primary Redundant: 127.10.20.30

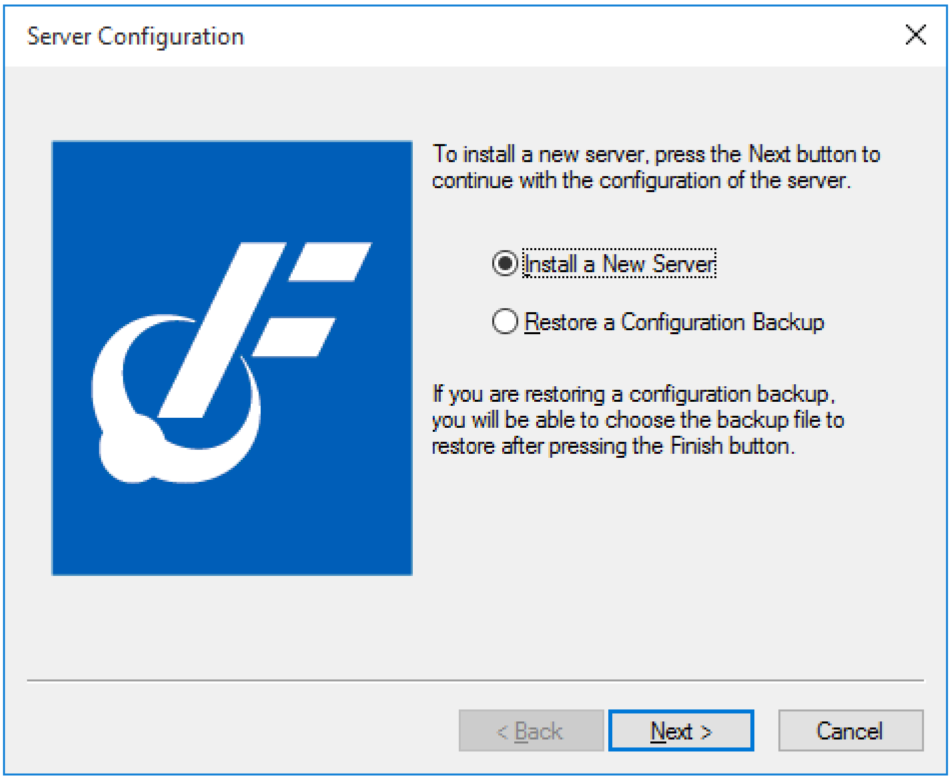
○ Secondary Redundant

Do not use 127.0.0.1 or any other form of loopback addressing. **This is not supported!**

Setting up a Redundant Server

Perform the following steps on the server that will be designated Redundant.

1. Create a new Foreseer server by launching the Foreseer application. Select Install New Server. Click Next to Continue.



Server Configuration

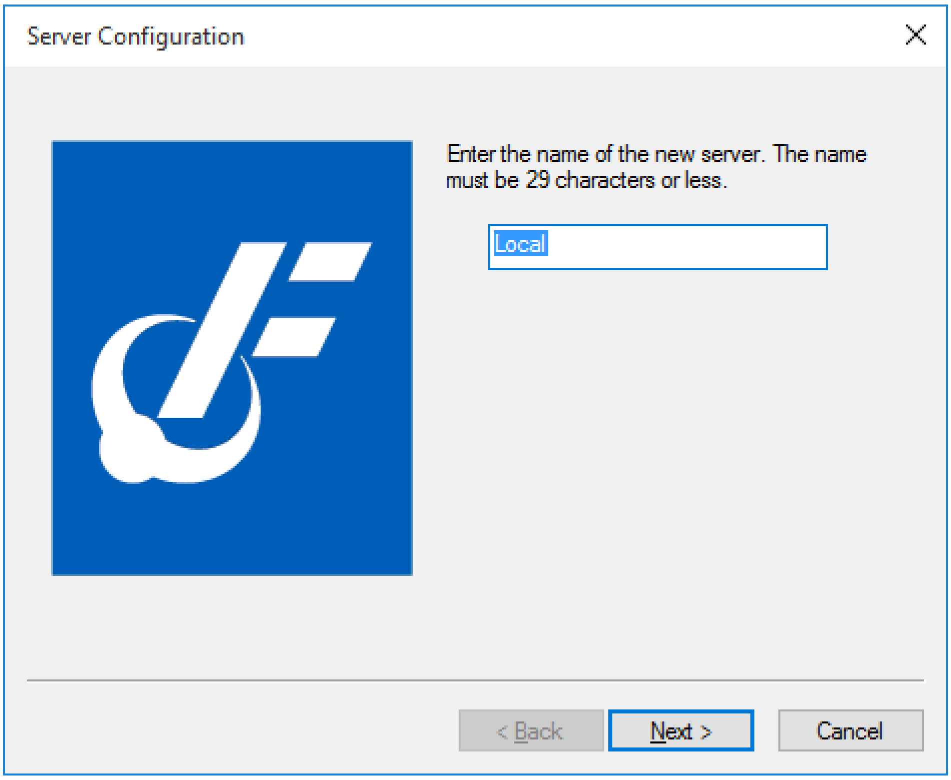
To install a new server, press the Next button to continue with the configuration of the server.

● Install a New Server

○ Restore a Configuration Backup

If you are restoring a configuration backup, you will be able to choose the backup file to restore after pressing the Finish button.

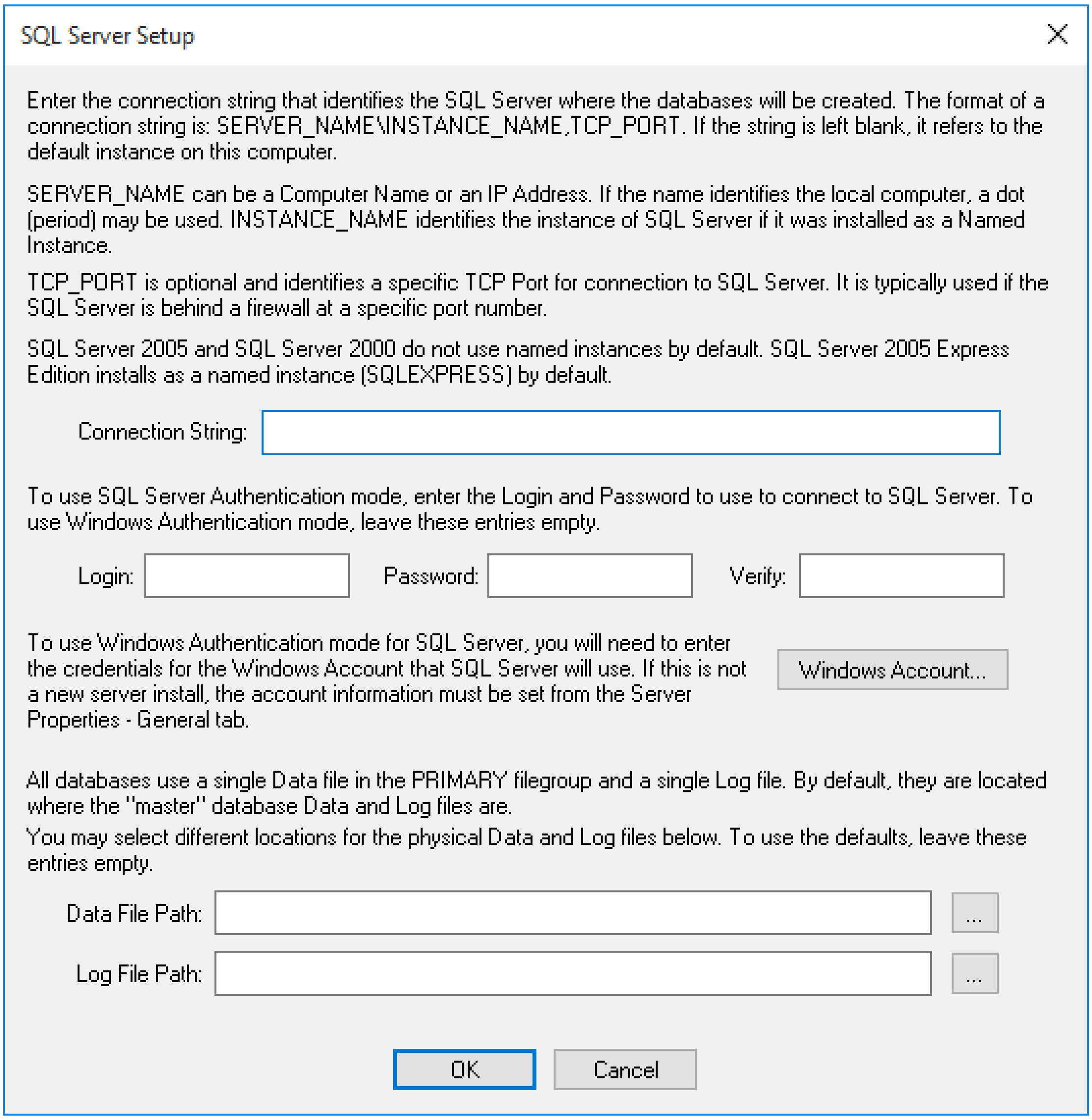
2. Enter the name of the server. This must be identical to the name on the primary server. Click Next to continue.



Enter the name of the new server. The name must be 29 characters or less.

Local

3. Enter the database information. The Redundant Server requires its own SQL Server Instance. The Primary and Redundant cannot use the same instance of SQL Server. Click Next.


SQL Server Setup

Enter the connection string that identifies the SQL Server where the databases will be created. The format of a connection string is: SERVER_NAME\INSTANCE_NAME,TCP_PORT. If the string is left blank, it refers to the default instance on this computer.

SERVER_NAME can be a Computer Name or an IP Address. If the name identifies the local computer, a dot (period) may be used. INSTANCE_NAME identifies the instance of SQL Server if it was installed as a Named Instance.

TCP_PORT is optional and identifies a specific TCP Port for connection to SQL Server. It is typically used if the SQL Server is behind a firewall at a specific port number.

SQL Server 2005 and SQL Server 2000 do not use named instances by default. SQL Server 2005 Express Edition installs as a named instance (SQLEXPRESS) by default.

Connection String:

To use SQL Server Authentication mode, enter the Login and Password to use to connect to SQL Server. To use Windows Authentication mode, leave these entries empty.

Login: Password: Verify:

To use Windows Authentication mode for SQL Server, you will need to enter the credentials for the Windows Account that SQL Server will use. If this is not a new server install, the account information must be set from the Server Properties - General tab.

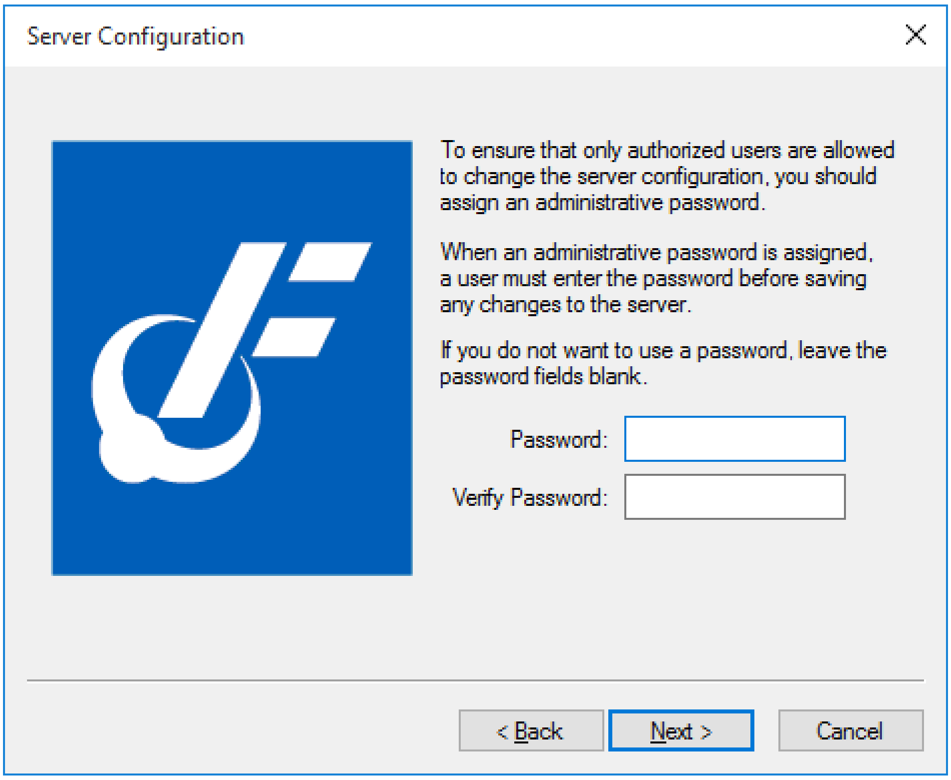
All databases use a single Data file in the PRIMARY filegroup and a single Log file. By default, they are located where the "master" database Data and Log files are.

You may select different locations for the physical Data and Log files below. To use the defaults, leave these entries empty.

Data File Path:

Log File Path:

4. Do not enter a password. If an admin password is used on the Primary Server, it will be set automatically once the redundant relationship has been completed. Click Next.



Server Configuration

To ensure that only authorized users are allowed to change the server configuration, you should assign an administrative password.

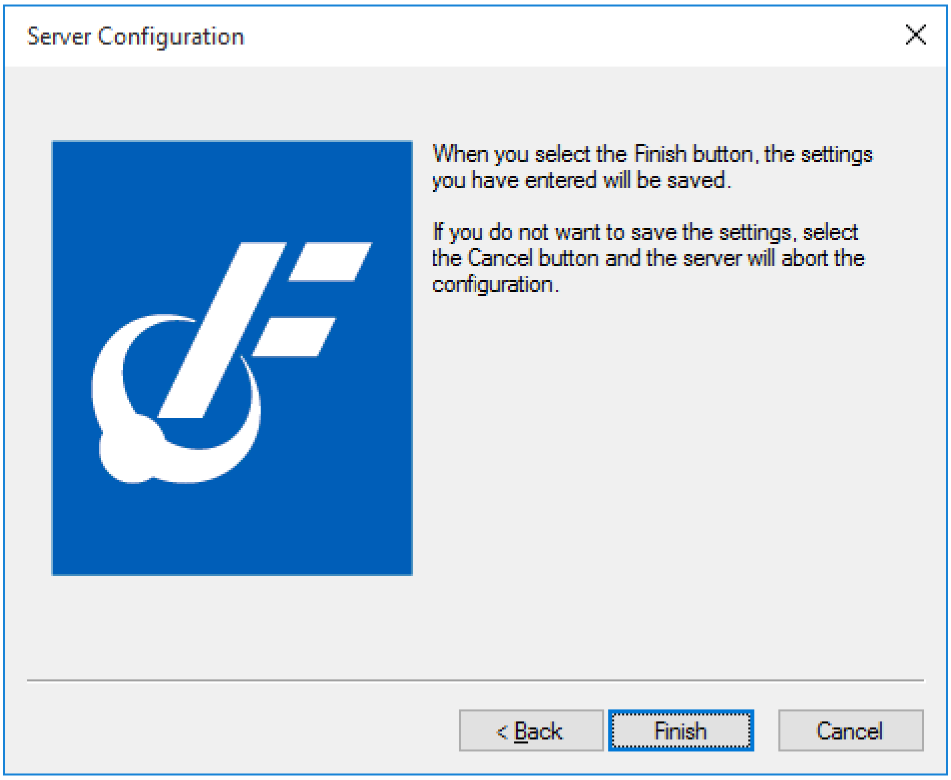
When an administrative password is assigned, a user must enter the password before saving any changes to the server.

If you do not want to use a password, leave the password fields blank.

Password:

Verify Password:

5. Click Finish to complete the Server Configuration wizard. This will create the new server configuration and Foreseer will finish launching as an application.

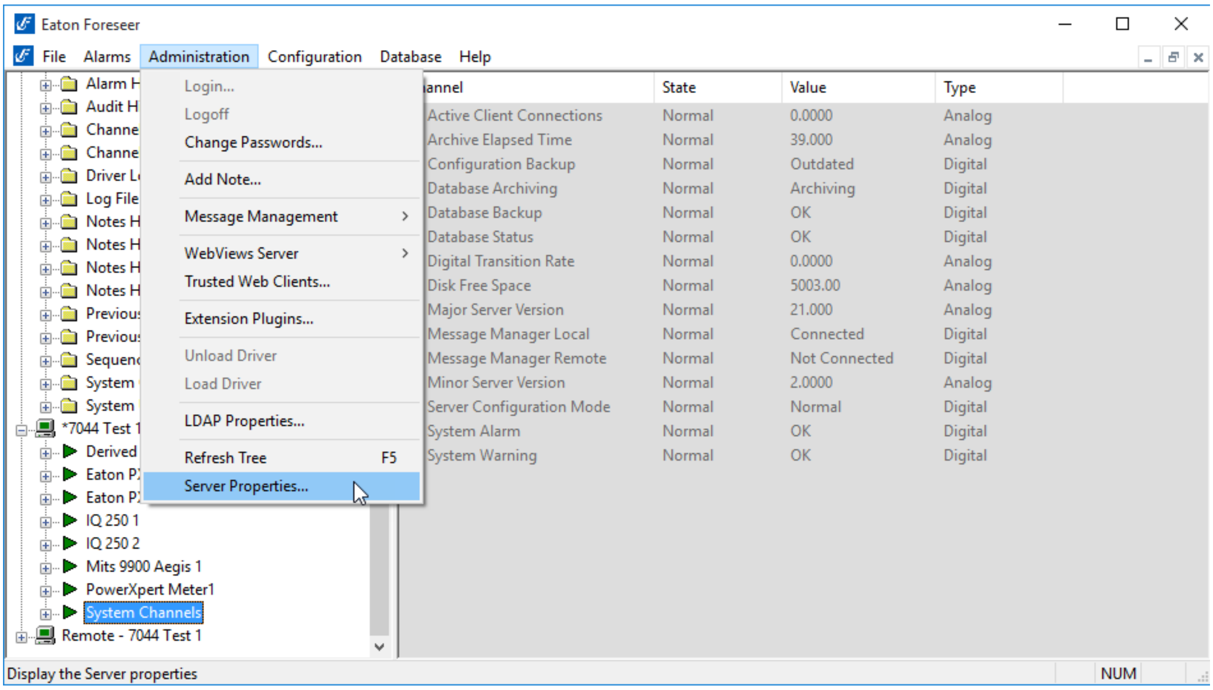


Server Configuration

When you select the Finish button, the settings you have entered will be saved.

If you do not want to save the settings, select the Cancel button and the server will abort the configuration.

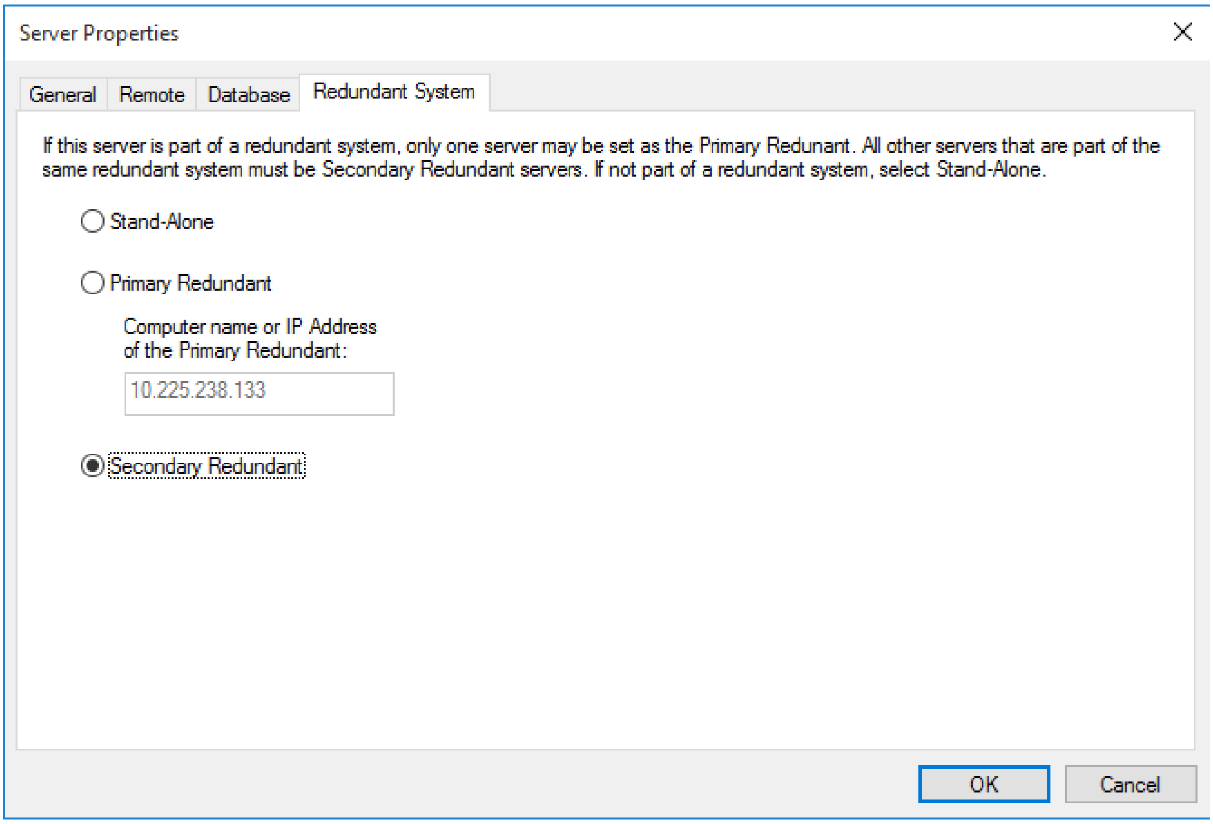
6. When the new configuration starts, access Administration>Server Properties.



annel	State	Value	Type
Active Client Connections	Normal	0.0000	Analog
Archive Elapsed Time	Normal	39.000	Analog
Configuration Backup	Normal	Outdated	Digital
Database Archiving	Normal	Archiving	Digital
Database Backup	Normal	OK	Digital
Database Status	Normal	OK	Digital
Digital Transition Rate	Normal	0.0000	Analog
Disk Free Space	Normal	5003.00	Analog
Major Server Version	Normal	21.000	Analog
Message Manager Local	Normal	Connected	Digital
Message Manager Remote	Normal	Not Connected	Digital
Minor Server Version	Normal	2.0000	Analog
Server Configuration Mode	Normal	Normal	Digital
System Alarm	Normal	OK	Digital
System Warning	Normal	OK	Digital

Display the Server properties

7. On the Redundant System tab, select the Secondary Redundant radio button. Click OK.



If this server is part of a redundant system, only one server may be set as the Primary Redunant. All other servers that are part of the same redundant system must be Secondary Redundant servers. If not part of a redundant system, select Stand-Alone.

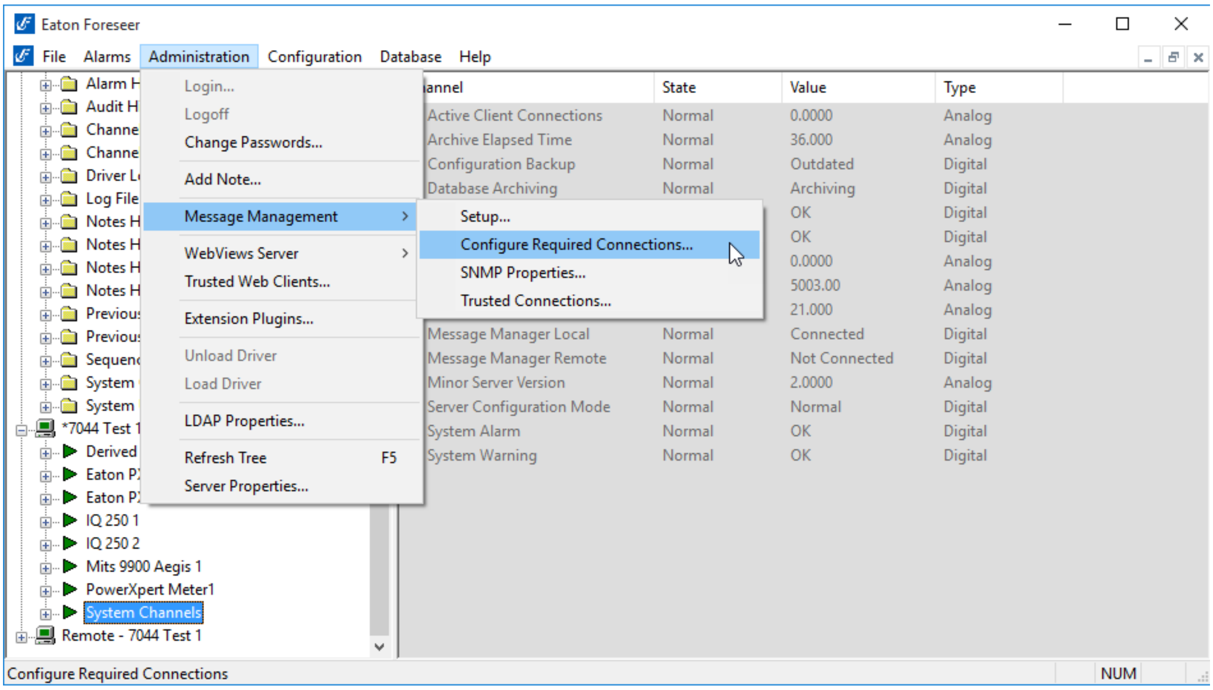
○ Stand-Alone

○ Primary Redundant

Computer name or IP Address of the Primary Redundant: 10.225.238.133

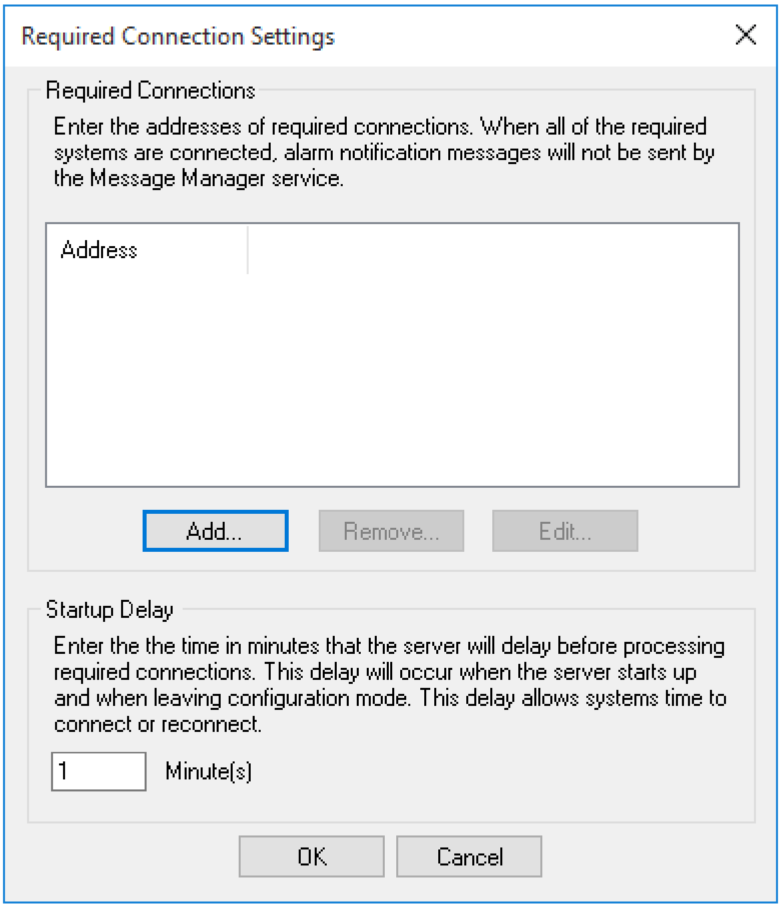
● Secondary Redundant

8. If the site is using Message Manager, select Message Management>Configure Required Connections...



annel	State	Value	Type
Active Client Connections	Normal	0.0000	Analog
Archive Elapsed Time	Normal	36.000	Analog
Configuration Backup	Normal	Outdated	Digital
Database Archiving	Normal	Archiving	Digital
		OK	Digital
		OK	Digital
		0.0000	Analog
		5003.00	Analog
		21.000	Analog
Message Manager Local	Normal	Connected	Digital
Message Manager Remote	Normal	Not Connected	Digital
Minor Server Version	Normal	2.0000	Analog
Server Configuration Mode	Normal	Normal	Digital
System Alarm	Normal	OK	Digital
System Warning	Normal	OK	Digital

9. On the Required Connection Settings dialog, click Add.


Required Connection Settings

Required Connections

Enter the addresses of required connections. When all of the required systems are connected, alarm notification messages will not be sent by the Message Manager service.

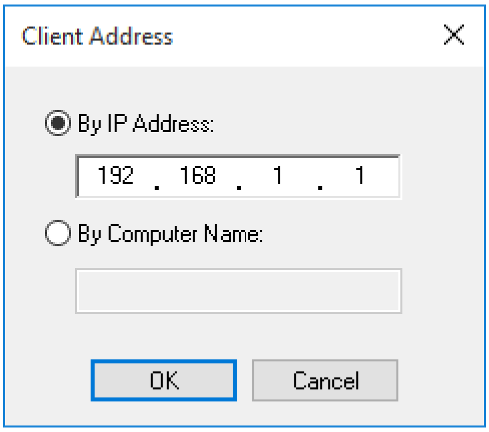
Address

Startup Delay

Enter the the time in minutes that the server will delay before processing required connections. This delay will occur when the server starts up and when leaving configuration mode. This delay allows systems time to connect or reconnect.

1 Minute(s)

10. Enter the Static IP Address or Resolvable Computer Name of the Primary Server. Click OK.



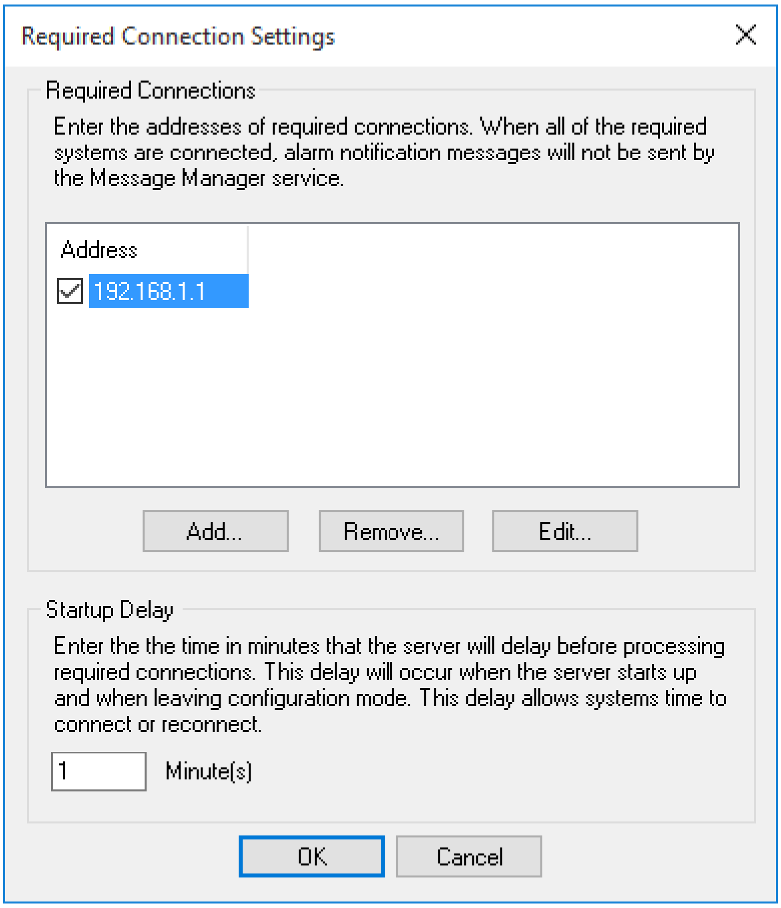
Client Address

● By IP Address:

192 . 168 . 1 . 1

○ By Computer Name:

11. Check the box next to the address to activate the setting for the Primary IP Ad- dress. You can also change the delay (1 minute is usually adequate). Click OKto save the changes. You may now shut-down Foreseer as an application andstart it as a service.



Required Connection Settings

Required Connections

Enter the addresses of required connections. When all of the required systems are connected, alarm notification messages will not be sent by the Message Manager service.

Address

☑ 192.168.1.1

Startup Delay

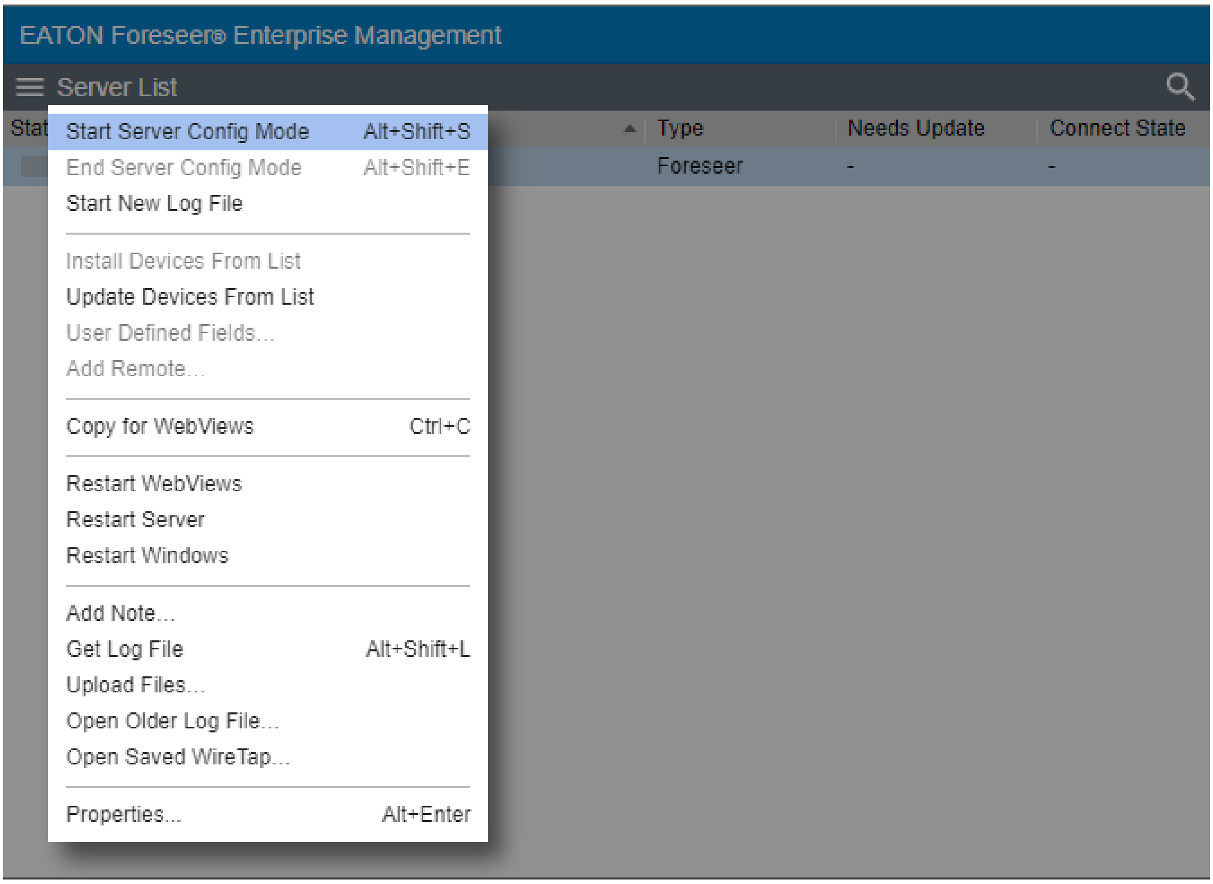
Enter the the time in minutes that the server will delay before processing required connections. This delay will occur when the server starts up and when leaving configuration mode. This delay allows systems time to connect or reconnect.

1 Minute(s)

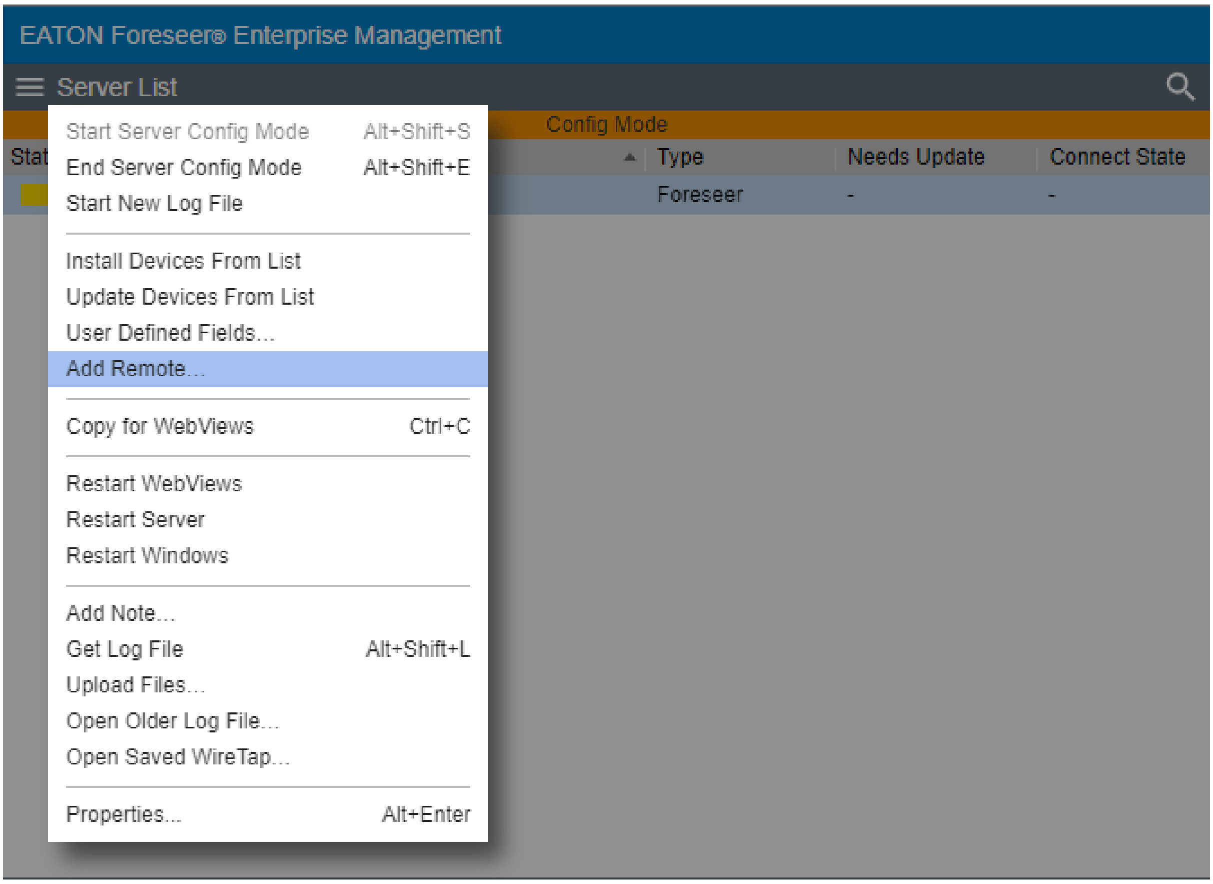
Adding The Redundant Server As A Remote On The Primary Server

The following must be carried out in the Primary Server using WebConfig. Ensure that the proper Windows groups are created and the required users are added.

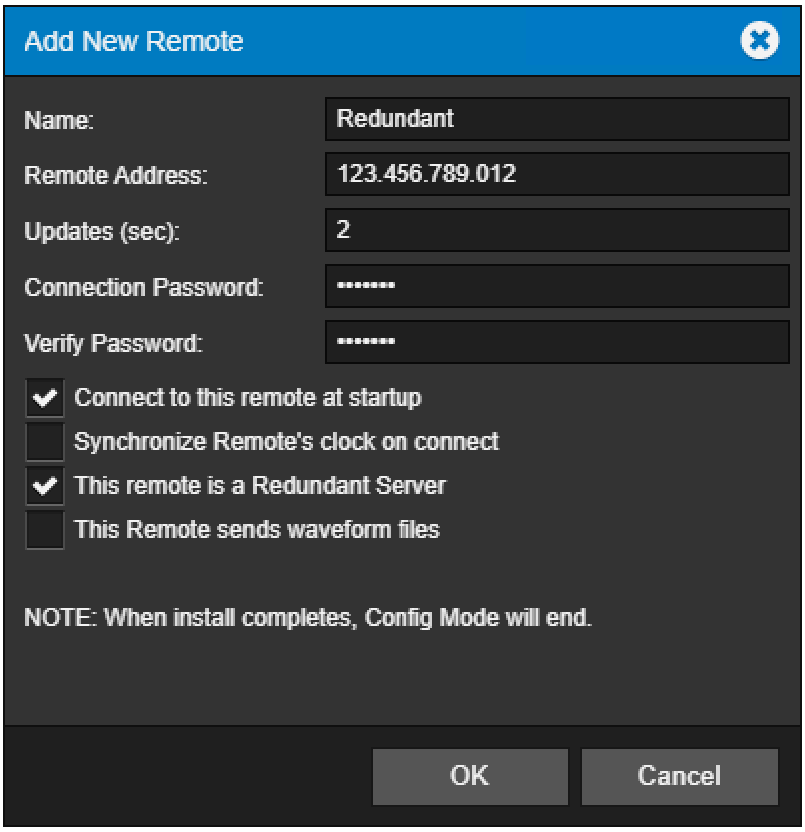
1. Select Start Server Config Mode from the WebConfig Server List menu.



2. Select Add Remote...



3. On the Pop Up window (Make sure pop-ups are allowed in Internet Explorer) Fill in the following information:
    1. Name – Must be named Redundant
    2. Remote Address – IP address of the Redundant Server.
    3. Updates – leave at 2 seconds.
    4. Connection Password – the default connection password is special
    5. (case-sensitive, all lower-caseletters).
    6. Verify Password – re-enter default connection password from step d.
    7. Check the “This is a Redundant Server” checkbox.Redundant



Name: Redundant

Remote Address: 123.456.789.012

Updates (sec): 2

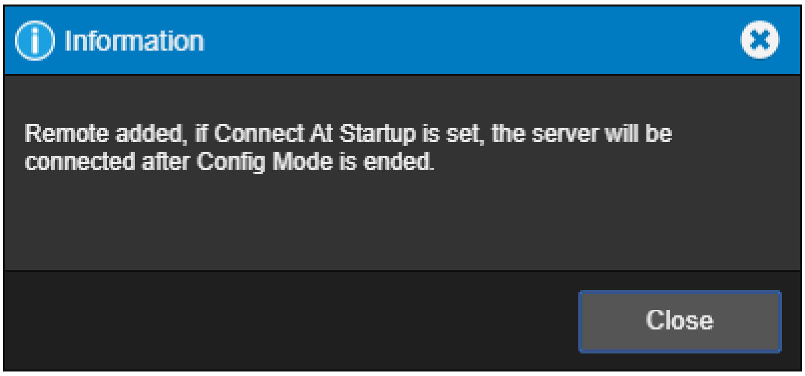
Connection Password: •••••••

Verify Password: •••••••

☑ Connect to this remote at startup
□ Synchronize Remote's clock on connect
☑ This remote is a Redundant Server
□ This Remote sends waveform files

NOTE: When install completes, Config Mode will end.

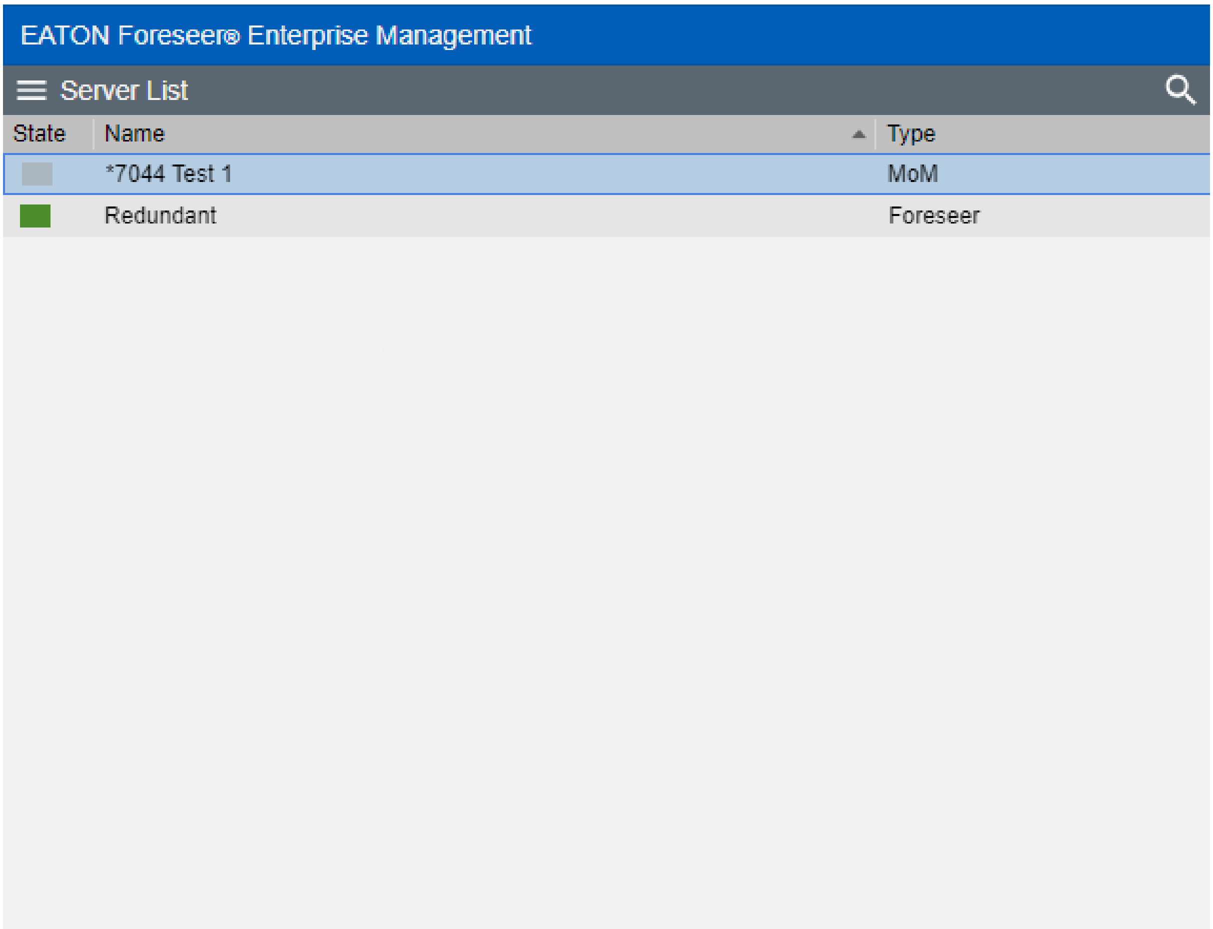
4. Click OK. The remote should be added to the server tree.



Remote added, if Connect At Startup is set, the server will be connected after Config Mode is ended.

If the process fails to add the Redundant server check the Windows Firewall settings to make sure that Port 2100, Port 2101, and HTTPS is open for traffic in both directions. You may need to temporarily turn Windows Firewall off to test. If the Redundant connects when the Firewall is off consult with the end customer for Firewall exceptions to be made.

5. End server configuration. In the right-side workspace of WebConfig, you should see that the Redundant is connected, but lists its Needs Update field as Needs Sync.



EATON Foreseer® Enterprise Management

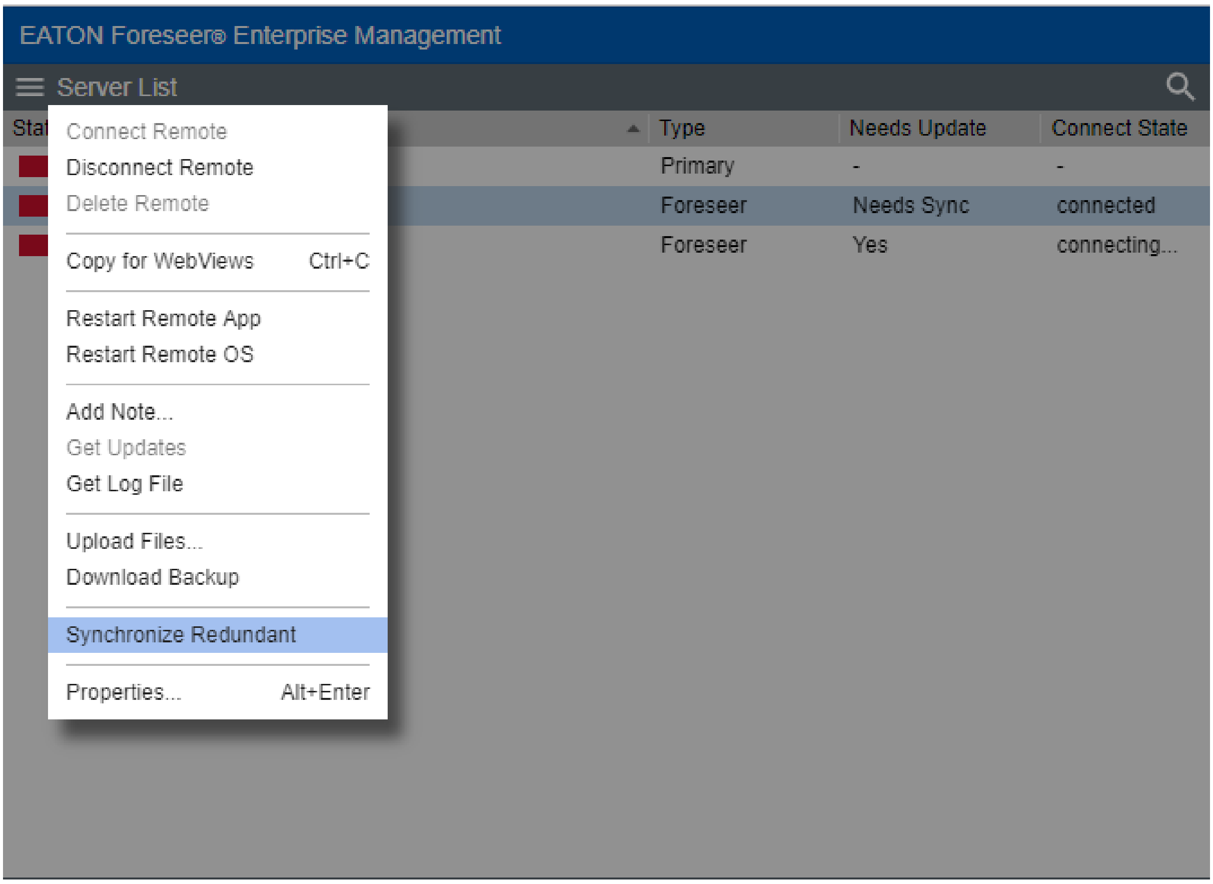
Server List

State	Name	Type
⬜	*7044 Test 1	MoM
🟩	Redundant	Foreseer

Synchronizing the Redundant Server

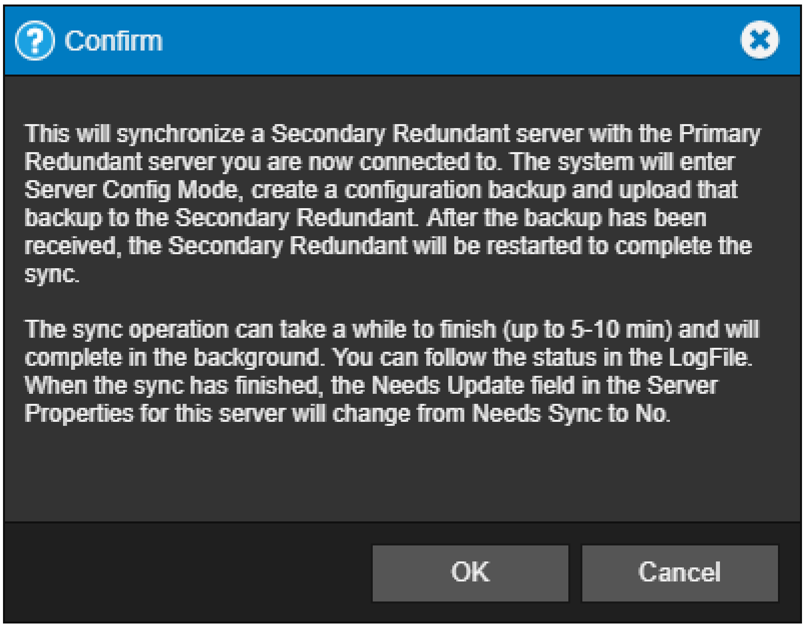
Not all changes on the Primary server will set the ‘Needs Sync’ flag under the ‘Needs Update’ header, typically channel properties will not but you can always per- form a synchronization to ensure the systems have identical settings.

1. Right click on the Redundant Server and select ‘Synchronize Redundant Server’.



Stat	Type	Needs Update	Connect State
🟥	Primary	-	-
🟥	Foreseer	Needs Sync	connected
🟥	Foreseer	Yes	connecting...

2. The following message will display. Click OK to continue.



This will synchronize a Secondary Redundant server with the Primary Redundant server you are now connected to. The system will enter Server Config Mode, create a configuration backup and upload that backup to the Secondary Redundant. After the backup has been received, the Secondary Redundant will be restarted to complete the sync.

The sync operation can take a while to finish (up to 5-10 min) and will complete in the background. You can follow the status in the LogFile. When the sync has finished, the Needs Update field in the Server Properties for this server will change from Needs Sync to No.

3. At this time a partial configuration backup is generated from the Primary server, transferred to the Redundant server and a restart of the Redundant server is initiated. The WebConfig tree will display a SYNC IN PROGRESS message. While this process is occurring, the WebConfig webpages may appear unresponsive. This is completely normal.
4. During the startup of the Redundant server an automatic database fix and check will

occur. This is performed to implement any changes to devices or channels that may have occurred on the Primary Server.

Both Servers should now be fully synchronized.

Add Remote Server

A local Foreseer Server can serve as host to a remote Foreseer Server. Once defined, the Remote Server appears on the Tree View as another computer and can be modified locally. A Password provision adds another layer of security by restricting access to authorized personnel.

To add and connect to a Remote Server, you will need to use the web configuration utility.

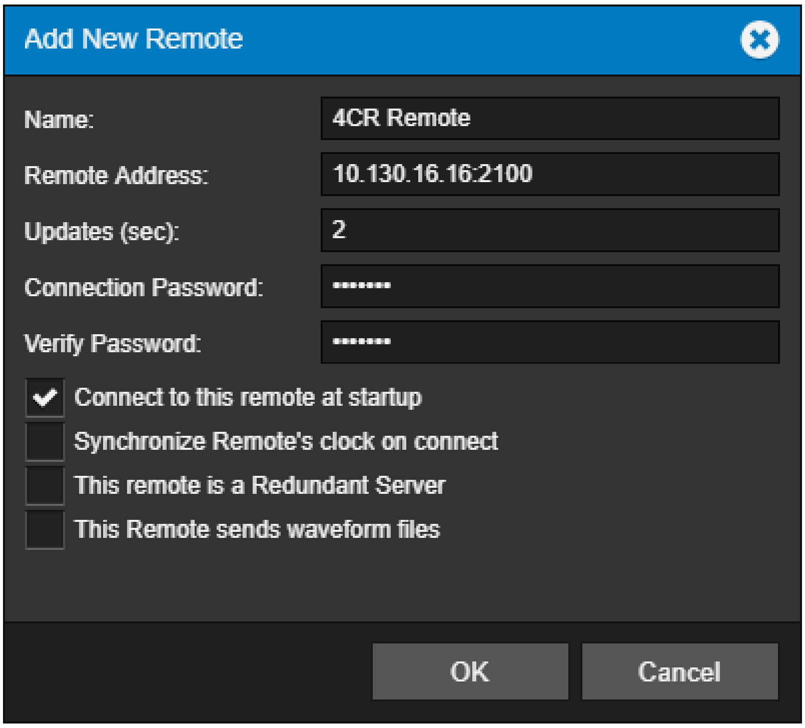
You can access the Web Configuration Utility at the following URL: https://*machine*/ Support/WebConfig.htm

Where *machine* is either the machine name or IP address of the machine on which Foreseer is installed. When accessing the web page, you may be challenged to pro- vide your user ID and password.

If you must designate a specific port for communicating with the WebViews server, the syntax of the URL will be slightly different:
https://*machine*:port_number/Support/WebConfig.htm
Server Config mode must be active to run this command. Activate Config mode by right-clicking server and selecting Start Server Config Mode. The **** CONFIG MODE **** message should be displayed above the tree.

To add a remote server:

1. Select Add Remote in the server right-click menu.
2. Identify the remote server by entering its Name and Remote Address; requiring Connection Password security is optional. If a password is specified for remote server access, the password must be entered a second time in the Verify Pass- word field. If no password is specified, it defaults to special.
3. Either accept the 2 second default for Updates (sec) or enter a new setting.



Name: 4CR Remote
Remote Address: 10.130.16.16:2100
Updates (sec): 2
Connection Password: •••••••
Verify Password: •••••••

☑ Connect to this remote at startup
□ Synchronize Remote's clock on connect
□ This remote is a Redundant Server
□ This Remote sends waveform files

4. Specify whether to automatically Connect to this Remote Server at startup and to Synchronize the Remotes clock on connect. You can also specify whether or not this server is redundant and if it sends waveform data.
5. Click OK and the Server attempts connection with the Remote Server. Once connection is established, the new Remote Server appears in the Tree View hierarchy.

Message Management Overview

Message Management establishes an automatic escalation procedure in response to user-specified alarms. When an alarm is detected, Foreseer proceeds to call each person in the appropriate notification list in the order shown until the alert is acknowledged. The **Status** portion of the **Message Management** window reports the notification is being performed and its ongoing progress. If everyone on the **List** is called without receiving an acknowledgment, Foreseer can repeat the entire procedure until the alarm is acknowledged, thereby ensuring a response. There are also provisions for suspending or stopping individual calls (as well as the entire notification procedure once it has been initiated) using the Message menu or the integral Messages tool-bar.

Message Management

✓ For more information, please refer to the: *Message Manager Configuration Guide (MN152112EN).*

Glossary

Ack Holdoff

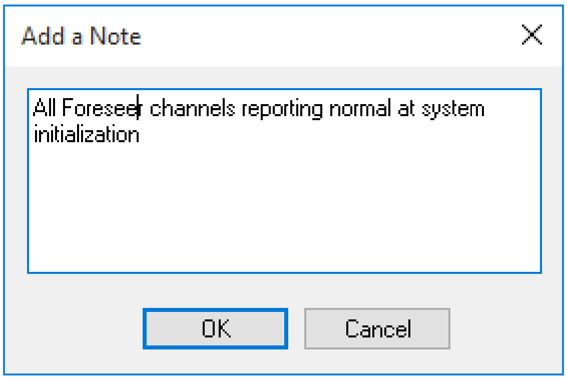
Ack Holdoff defines (in minutes) the delay interval after a channel alarm has been acknowledged (or silenced) before it is automatically rearmed. Acquired data continues to be displayed, but the channel's Current Value is no longer compared to its defined Alarm Limits. The default Holdoff period of one hour may be manually overridden at any time using the Foreseer Client's Rearm command, or when the alarm is acknowledged.

Add Button

Add includes the currently highlighted item(s) in the selection list.

Adding Notes

The Foreseer **Notes** feature fulfills a unique and timely function by recording any supplemental information relevant to a particular event when it occurs. Simply choose the Add Note... command in the Administration menu. The **Add a Note** dialog box permits the System Administrator to enter **Notes** which are logged into the Server's database and can be reviewed by authorized Foreseer Clients or retrieved in Foreseer Reports. An unlimited number of real-time **Notes** may be entered, but they are limited to 255 characters each. Foreseer **Notes** can also be entered in the course of Acknowledged and Rearming alarms.



All Foreseer channels reporting normal at system initialization

Address

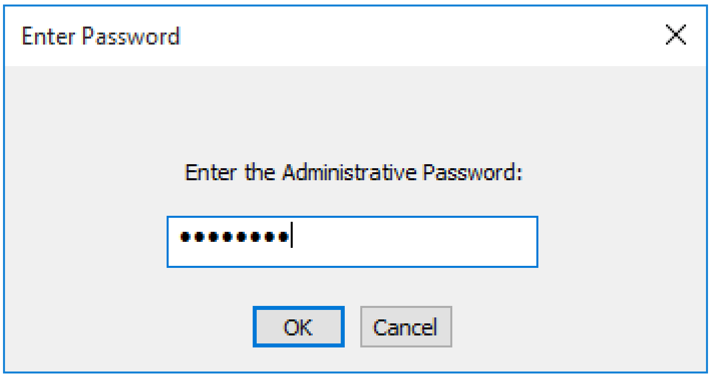
Address is the target device's IP Address in a network installation. This Address ***must*** be correct or network connections cannot be established between the Foreseer Server and the target Device.

Add Slave

Includes the identified Slave Server Name in the associated list box for Heartbeat function.

Administrative Authorization

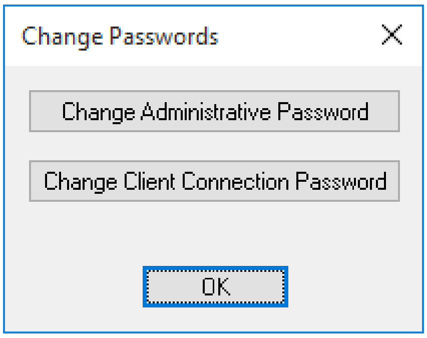
Password protection ensures that only authorized personnel are allowed to alter the Foreseer Server configuration or halt its data gathering and system monitoring operations. When enabled, a security password must be entered before most Server functions can be accessed. The first attempt to alter protected Server settings requires the **Administrative Password**. The password is entered in the **Administrative Password** dialog box; asterisks are displayed to maintain system security. The accepted entry automatically becomes part of the System Log and is available for review in that Foreseer Report. Once entered, the user has access privilege to all protected Server functions and does not have to enter the password again during the current session.



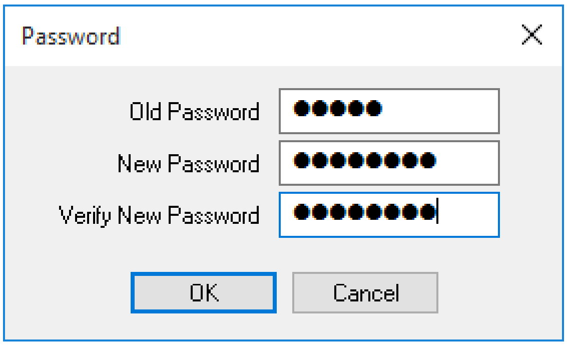
The Administrative and Client Connection Passwords may be changed, or assigned at a later time if one was not specified during initial Server configuration. The **Change Passwords** dialog box permits these Foreseer Server authorizations to be altered. Changing a Password does require entry of the Old password before you are allowed access the New password field.

To change the Server's current Administrative password:

1. Select Change Passwords... under the Administration menu and the **Change Server Password** dialog box is displayed.


Change Passwords
Change Administrative Password
Change Client Connection Password
OK

2. Click on the Change Administrative Password or the Change Database Password button to display the appropriate dialog box.



3. Enter the Old Password; asterisks are displayed to maintain system security. If no Password was previously assigned, simply **Tab** to the New Password field.
4. Enter the desired New Password.

✓ Passwords are case-sensitive; therefore "USER," "User" and "user" are all recognized as different Passwords.

5. Type the same character string in the Verify New Password field to validate the New Password.
6. Click OK to save the New Password.

Agent DLL Directory

Is the directory location within the Server PC of the installed SNMP Agent, typically the Foreseer folder.

Alarm Events

Determines when the specified Critical Alarm and Cautionary Alarm Traps are sent to the supervisory NMS in response to a Limit excursion detected on this channel.

Alarm Message

Is the display text corresponding to the channel's Cautionary (yellow) and Critical (**red**) Alarm Limits, if Enabled. Messages may be independently assigned to the Hi and Lo Limits for each *Meters* (analog) channel level event. A *Status* (digital) channel can have only one Message.

Alarm on Value

Specifies whether a False (0) or a True (1) value triggers an alarm for this digital channel.

Alarm Type

Specifies whether an alarm reported on this channel represents a Cautionary (**yellow**) or a Critical (**red**) Alarm Limit excursion.

Alarm Updates

Specifies how often the <Alarm Management> display is updated with alarm information from the Remote Server

Alpha Message

Allows you to identify the type of message that is to be sent with the alert issued when an alarm is reported on this channel and is the normal *Message Management* notification method. A Standard Alarm Message is specified in the channel's *Meters* (analog) or *Status* (digital) **Basic Properties** dialog box and applies to **Critical** and **Cautionary** alarm conditions. The message "Acknowledged" is automatically sent for an **Acknowledged** state and "Channel Normal" for a **Normal** state. Checking the appropriate boxes also includes the Server, Device, Channel Name and/or Alarm Message. You can enter an additional Alpha Message to Include in the notification as well asthe alarm message. Selecting *Edit the Custom Message* opens a dialog box allowing alternative response instructions to be entered.

Apply

Enables the COM Port Settings shown. This command can be used to verify communications with the Foreseer Server and before proceeding with **Device Installation**.

Archive

Specifies the analog channel Value that is archived to the Foreseer Server database. It may be the AVERAGE, or the MINIMUM, MAXIMUM, FIRST, LAST, NULL or NONE reading over the archive interval.

Available Time

Specifies when the named Subscriber is available for paging by designating the Start and

End Time which define the period that person can be notified. Enter the times or use the associated arrows to scroll to the appropriate Time. The corresponding display changes to report the total Availability Time.

Baud Rate

Is the data transfer rate between Foreseer and the messaging device. Other Rates are available by pressing the associated arrow. The Baud Rate is available from the device's manual or the service company.

Bits Per Second

Is the baud rate transmitted through the serial interface each second. Other Bit selections are available by pressing the associated arrow.

Border Display

Determines the type of Border used to delineate the data in the Browser display. You may wish to try all three settings to determine which looks best on the Browser(s) accessing the Web Server.

Browser Format

Determines how the Web Server data is displayed. Browser Based, the default, attempts to determine the type of Browser on-the-fly and present the Web Server information in an appropriate format. This setting is particularly useful in instances where the Server may be accessed by multiple Browser types and should only be changed if all potential Web Browsers use the same format.

Call Again

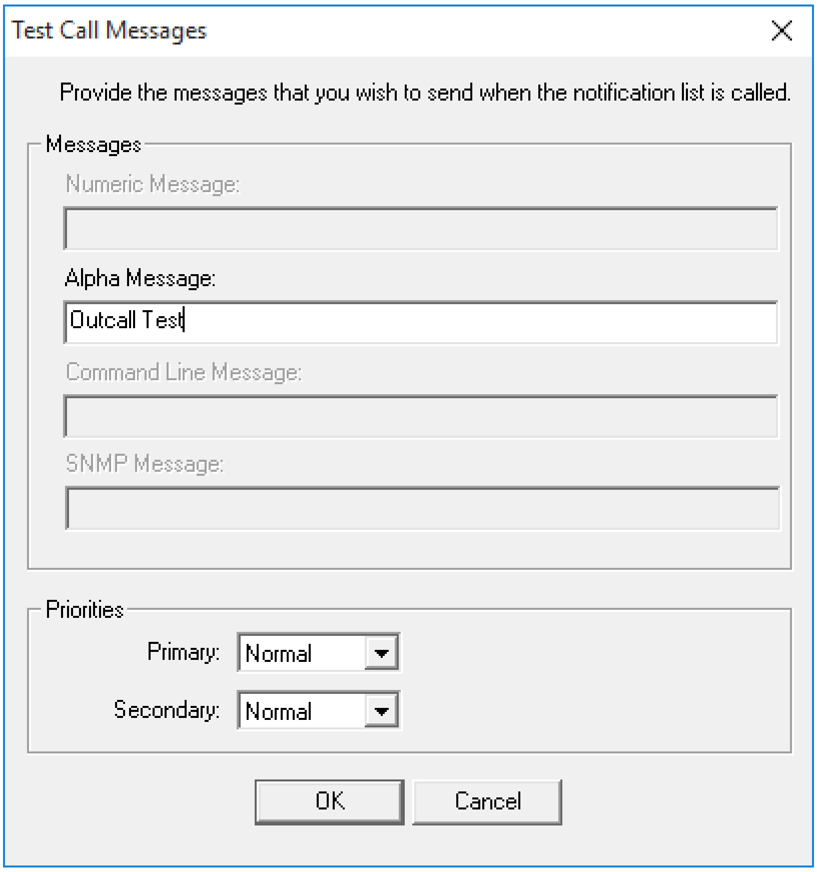
Re-initiates the call highlighted in the **Status** area of the *Message Management* window.

Call Entries

Specifies the length of time recorded messages are kept before being automatically deleted from the list.

Call Now

The **Call Now** dialog box, displayed when the Test Call button is pressed in the *Notification Lists* window, allows you to verify that *Message Management* notifications are performed properly.



Provide the messages that you wish to send when the notification list is called.

Alpha Message: Outcall Test

Primary: Normal

Secondary: Normal

Call Properties

Determine whether to call the entire **Notification List** even if an alarm acknowledgment is received and messaging is terminated, allow higher priority**Lists** to take call precedence, and if listed personnel using the same *Service* should be notified with the same call.

Cancel Button

Exits this dialog box without making any changes.

Cautionary Alarm Trap Numbers

The number of the Trap, ranging from 200-224 in the Foreseer SNMP Virtual Agent, that will be sent to the Network Management System (NMS) in response to a Cautionary Alarm for this channel.

Channel Disabled

When checked, alarms are not reported and data is not archived for this channel. Disabling a channel is useful when performing Device maintenance or making repairs to avoid archiving inappropriate readings.

Channel Disarmed

When checked, suspends alarm reporting for this channel. Data, however, continues to be archived. Disarming a channel is useful when performing Device maintenance or making repairs to avoid reporting nuisance alarms.

Channel State

Is a fixed entry reporting the current alarm status of the input as Normal, Cautionary, Critical or Acknowledged.

Channel Updates

Specifies how often the <Alarm Management> display is updated with channel information from the Remote Server.

Channel Value

Reports the result of *Testing* the displayed Equation.

Characters per Message

Is the maximum number of characters allowable in the paged message. Consult the pager manual or the paging company for the limitation of the device.

Classic Web Server

Foreseer offers browser access to WebViews via the WebViews Server. This Web Server can be defined to use either the HTTP or HTTPS protocols. Both can require User Name and Password authentication for access, but the HTTPS protocol furnishes an additional layer of security by protecting the transmission of information between the Client and the Server.

Safeguarding the information stored in the Foreseer Server database while allowing Internet access can present problems if the data is sensitive. Increasingly, business organizations are using digital Server Certificates ensure confidential communications between the Server and Client. Foreseer has implemented a Secure Sockets Layer (SSL) protocol which can be used to authenticate both Client and Server, as well as encrypting the information they exchange through the HTTPS Server feature.

User authentication and access control historically are based on a name/password scheme. But this approach requires management of a name/password database and provides limited security. A digital Certificate is a type of identification in the form of a data file that links an organization's identity to their ownership of a Public Key. This Public Key, embedded in the Certificate , is uniquely linked to a corresponding Private Key Password to which only the owner of the Certificate has access. The two Keysand the corresponding Certificate are used not only for user authentication and access control, but also for such security measures as message integrity. Such an approach affords a secure form of authentication on both ends of the connection, ensures private communications.

Certificates of Authentication can be self-signed or purchased from a third-party source, depending on individual corporate policy. Third-party Certificate Authorities specialize in Certificate issuance and subsequent management. They take responsibility for ensuring that the company requesting the Certificate actually is the company it claims to be, as well as verifying anyone attempting to access the resident database.

Use of the HTTPS protocol requires a Private Key Password and a Server Certificate. Both are files that are created when a random 1024-bit number is generated as the Private Key Password, and both must be present on the Server to allow secure HTTPS access. A utility (openssl.exe) is provided in the Server folder for generating the Private Key Password (KEY) and a Certificate Signing Request (CSR) which can be used to obtain a Certificate of Authority from a reputable security firm, in this example VeriSign.

The Server Certificate utility provided with Foreseer is a command line tool which runs as a command prompt. You can also generate a self-signed Certificate for temporary use while you are waiting to receive your official certificate from a Certificate Authority. It can be re-issued, if necessary, after 30 days.

Classic Web Server - Alarm Details

The **Alarm Details** page summarizes the alarm condition and allows (authorized) Users to Acknowledge and/or Rearm the errant channel.

Classic Web Server - Alarms Page

The **Alarms Page** displays all Devices (and channels) on the Web Server with currently active alarms, as well as the highest reported alarm state of each. The Devices are sorted alphabetically by default, but can be sorted by other criteria by clicking on the appropriate header. For example, clicking on the **S** header sorts the list by highest alarm State. Each listed Device is an active link to an Alarm Details page; clicking on the other navigation buttons opens their respective pages.

Classic Web Server - Devices Page

The **Devices Page** displays all Devices currently configured on the Web Server as well as the highest alarm state of each. The Devices are sorted alphabetically by default, but can be sorted by other criteria by clicking on the appropriate header. For example, clicking on the **S** header sorts the list by highest alarm State. Each listed Device is an active link to its constituent channels; clicking on the other navigation buttons opens their respective pages.

Classic Web Server - Home Page

A Foreseer Server can be configured for access through the World Wide Web (WWW) to permit remote viewing of Device Status and Channel Values, as well as allowing limited **Report** and **Alarm Management** capabilities. Most Web Browser formats are accommodated by this function, but the Server first must be configured for HTTP or HTTPS Service.

Once configured, you can view a Foreseer or EnterLink Server through a Web Browser, simply by entering its IP Address as the URL or Web Address. For example, if the Server's IP Address is 204.144.132.2, you would enter http://204.144.132.2 to access its **Home Page**.

The **Home Page** contains a navigation buttons with links to the following subordinate pages:

Home returns to the **Home Page**.

Devices displays all Devices configured on the accessed Web Server and their current status.

Alarms displays all currently active alarms for on Web Server.

Reports allows Foreseer **Reports** to be Run and Retrieved.

The Enable/Disable Refresh button (when available on the Web Browser) updates the display at the Refresh Interval specified in the General **Web Server Properties** dialog box.

The **Home Page** may be customized by those who are familiar with the syntax using an HTML-compatible or simple text editor. If you are monitoring multiple Servers, for instance, you may wish to establish hypertext links to the other sites.

CAUTION: **Do not** modify the **Home Page** navigation button positions or you could disrupt the links to the other pages.

Classic Web Server - Reports Page

The **Reports Page** displays all currently available Foreseer Reports on the Web Server. The Reports are sorted alphabetically with the last three Reports available for viewing simply by clicking on them. Clicking on the Report Type runs a new Report of that Type (the oldest being discarded); clicking on the other navigation buttons opens their respective pages.

Classic Web Server - Servers Page

The **Server Page** displays all currently configured Foreseer Servers as well as the highest alarm state of each. The Servers are sorted alphabetically by default, but can be sorted by other criteria by clicking on the appropriate header. For example, clicking on the **S** header sorts the list by highest alarm State. Each listed Server is an active link to its resident Devices; clicking on the other navigation buttons opens their respective pages.

Close Button

Shuts this dialog box and retains the displayed settings.

Command Line

Is the command to execute for this user-defined Service. For example, entering C:exe (or simply Notepad.exe if the application is in the search path) would launch Windows Notepad program.

Communication Retries

Is the number of times communications are attempted when a Device command is unsuccessful.

Community Names

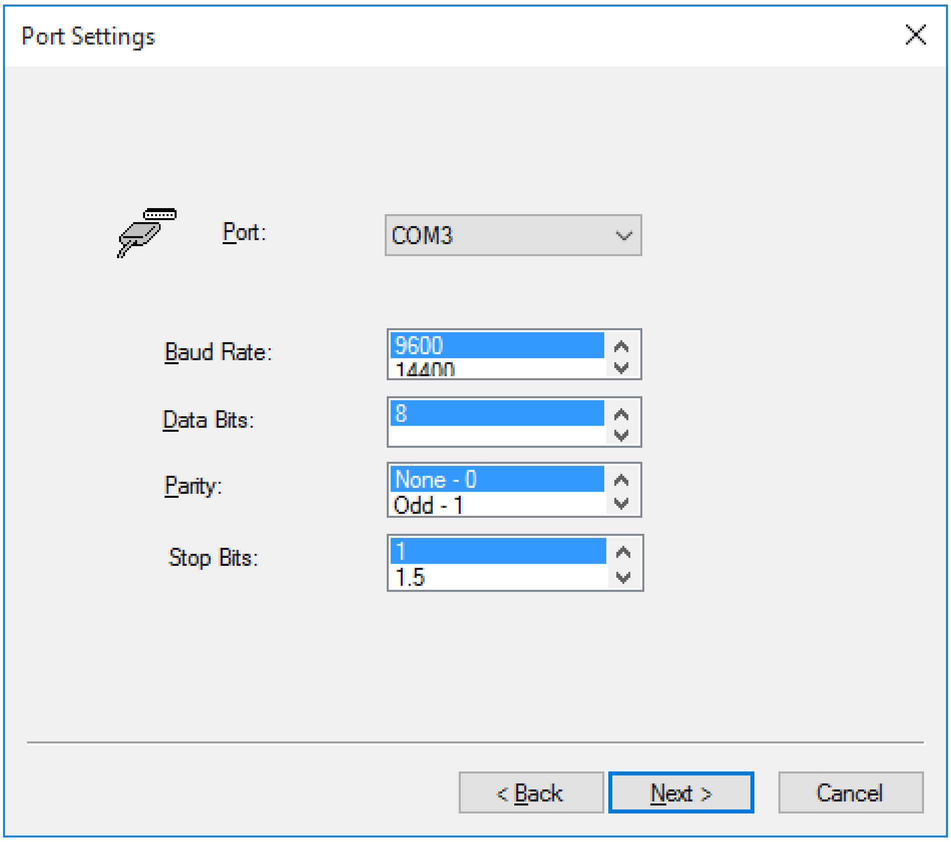
Is the list of Communities to receive Foreseer SNMP traps.

COM Port

Is the Foreseer Server serial port through which Device or TABS communications are sent. An alternate Port may be chosen from those available in the associated drop list. When installing devices, clicking on the Configure... button in the **COM Port Service Properties** dialog box displays the COM Properties dialog box, allowing these communications settings to be changed.

COM Properties

The **COM Properties** dialog box defines the communications parameters between the Foreseer Server and a directly connected serial Device. These variables ***must*** agree with the settings on the target Device or communications cannot be established.



Port Settings

Port: COM3

Baud Rate: 9600
14400

Data Bits: 8

Parity: None - 0
Odd - 1

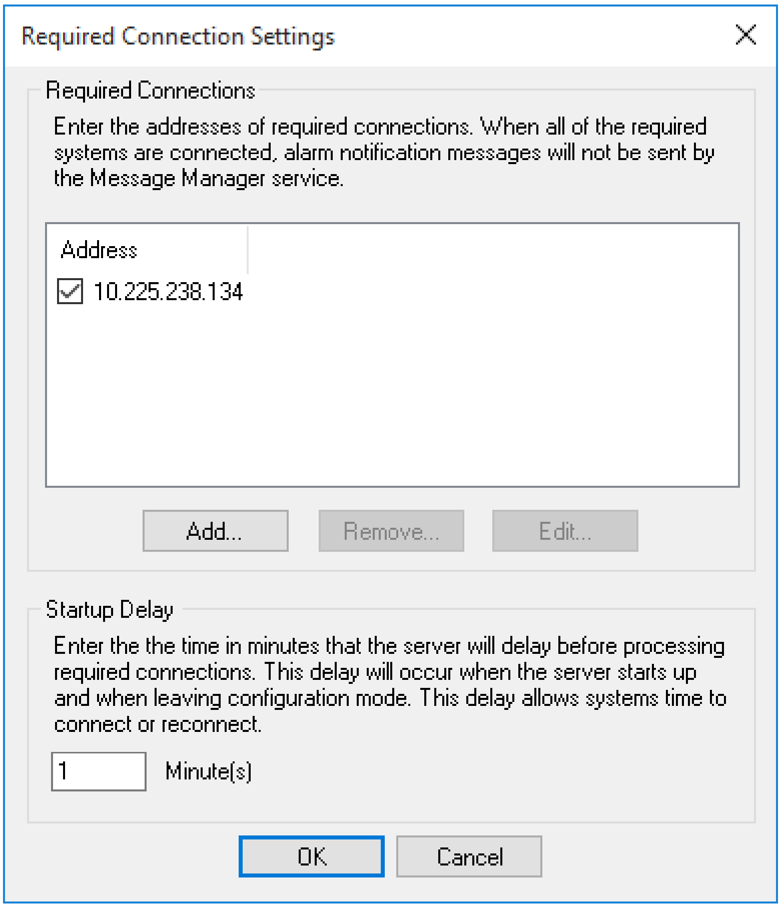
Stop Bits: 1
1.5

Configure Required Connections

This optional notification configuration procedure identifies which Foreseer Clients and/or Remote Servers are required to be connected to this Server to perform Message Management functions. If any one of the listed Servers or Clients becomes disconnected from this Server, the Message Management option begins its messaging routine to alert personnel of alarms.

To configure required connections:

1. Select the Configure Required Connections... command from the Administration menu **/** Message Management> sub menu to display the **Required Connection Settings** dialog box.



Required Connection Settings

Required Connections

Enter the addresses of required connections. When all of the required systems are connected, alarm notification messages will not be sent by the Message Manager service.

Address

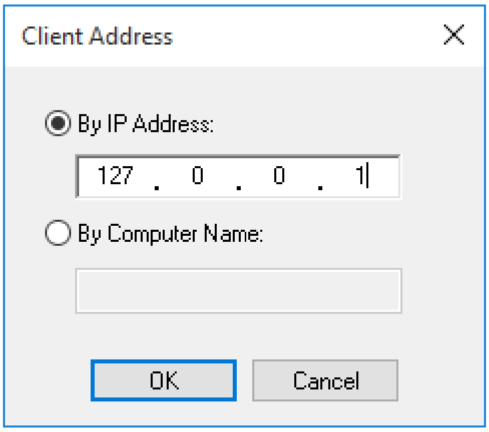
☑ 10.225.238.134

Startup Delay

Enter the the time in minutes that the server will delay before processing required connections. This delay will occur when the server starts up and when leaving configuration mode. This delay allows systems time to connect or reconnect.

1 Minute(s)

2. Click on the Add... button to access the **Enter Client IP Address** dialog box.



Client Address

● By IP Address:

127 . 0 . 0 . 1

○ By Computer Name:

3. Furnish the network Address or Computer Name. By IP Address is used for network connections to a fixed Server (the default of 127.0.0.1 is reserved for Foreseer Servers and Clients which are installed on the same PC); By Computer Name allows you to dynamically connect to a Client computer which does not have a fixed Address. Click OK to continue.
4. Check the box preceding the Address to enable Server access by that connection.
5. Specify the Startup Delay in which the Server will ignore any Remote Servers or Clients that become disconnected before initiating messaging. This Delay is in effect whenever the Server is initialized or when modification are made.
6. Repeat the process to Add... other Foreseer Clients or Remote Servers to the list.

7. Click OK to accept the displayed **Required Connection Settings** and return to normal operation.

Connection Password

Is an optional level of security which requires aPassword in order to access a Remote Server. The Password must be entered a second time to Verify it.

Connection Time-out

Specifies how long before connections with the Remote Server time-out.

Connect to this Server at Startup

Automatically initiates connection with this Remote Server when the ***Foreseer Server Application*** is launched.

Connect UPS is a registered trademark of Powerware Corporation

ConnectUPS(R) is a registered trademark of Powerware Corporation.

Contact

Is the name of the person in charge of the Foreseer SNMP interface.

Copy Button

Duplicates the selected Foreseer object(s) on the clipboard.

Copy Messages

Copies the information displayed in the Messages for Message Caller list box to the clipboard for printing or incorporation into other applications.

Copy These Settings to Other Dialog Tabs

Saves time and reduces the potential for data entry mistakes by pasting the messaging parameters shown under this tab in the *Channel Message Settings* dialog box into the chosen tab(s). This shortcut is recommended *only* for tabs that share the same messaging properties.

Create New Folder

Creates a new folder within the current Windows directory in which the specified File name will be saved.

Critical Alarm Trap Numbers

The number of the Trap, ranging from 200-224 in the Foreseer SNMP Virtual Agent, that will be sent to the Network Management System (NMS) in response to a Critical Alarm for this channel.

Current Device Settings

Identify the communications parameters between Foreseer and the connected Device. Note that these Settings cannot be modified from within the read-only**Device Properties** dialog box.

Current Value

Is a fixed entry showing the channel's last reported reading.

Database Administrative Account Name

Is the name of the Account Administrator used to access the SQL Database Server for configuration modification. The Name should remain blank for standard Windows Authentication. The administrative Account Name Password used to access the SQL Database Server is independent of the *Administrative Password* and can be altered by clicking on the Password button.

Database Backup

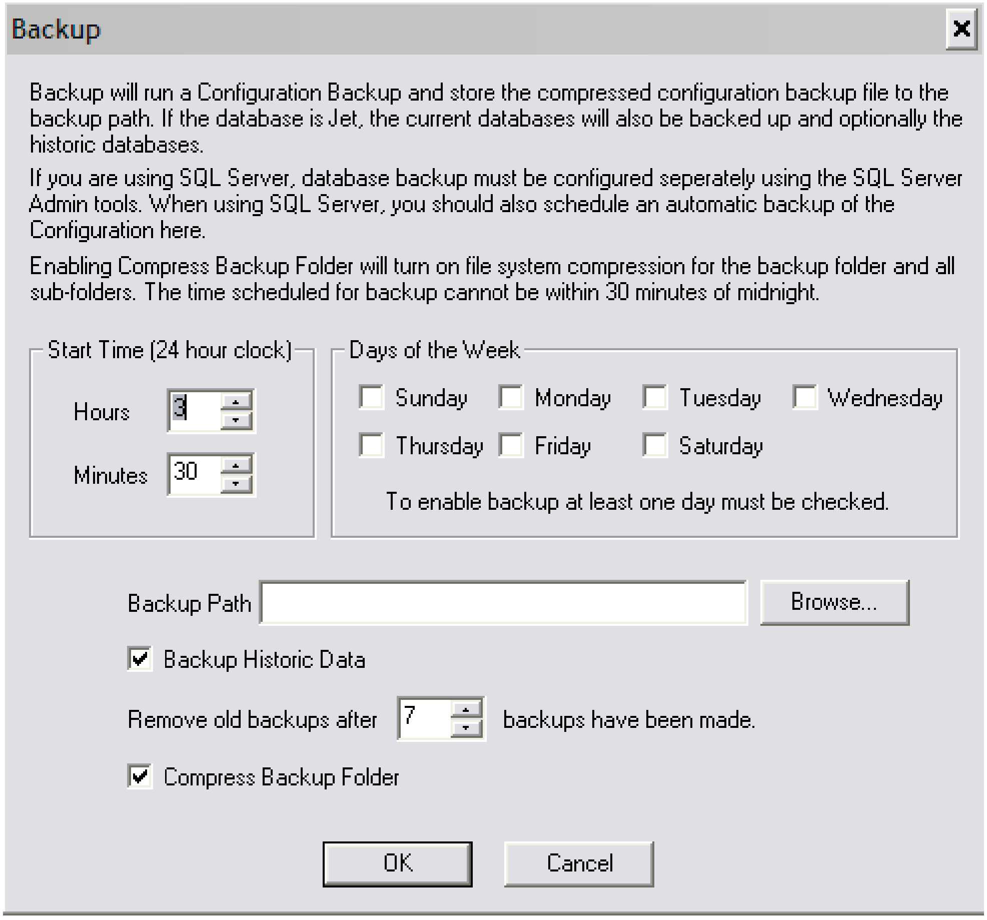
The Foreseer Server's archived database can be scheduled to be backed up automatically at specified intervals. The size of the Server database is determined by the number of channels and the rate at which the data is archived. A network drive is the recommended backup destination. The Backup archive includes Foreseer data files as well as logged **Alarms** and **Notes**, but does not include Server configuration information. Note that the use of the Jet database is now deprecated.

(see Configuration Backup).

To schedule a Foreseer Server Database Backup of a Jet database:

Administrative Authorization is required to backup the Server database. SQL Server databases are archived according to individual company protocols--consult your Network Administrator for instructions.

1. Select Database Backup... in the Database menu to display that dialog box.



Backup

Backup will run a Configuration Backup and store the compressed configuration backup file to the backup path. If the database is Jet, the current databases will also be backed up and optionally the historic databases.

If you are using SQL Server, database backup must be configured seperately using the SQL Server Admin tools. When using SQL Server, you should also schedule an automatic backup of the Configuration here.

Enabling Compress Backup Folder will turn on file system compression for the backup folder and all sub-folders. The time scheduled for backup cannot be within 30 minutes of midnight.

Start Time (24 hour clock)

Hours 3

Minutes 30

Days of the Week

□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday

To enable backup at least one day must be checked.

Backup Path

☑ Backup Historic Data

Remove old backups after 7 backups have been made.

☑ Compress Backup Folder

2. Specify when the backup is to be performed. The Start Time is based on a 24-hour clock: for example, 5:00 p.m. is entered as "17:00." Note that the backup cannot occur within ten minutes of midnight and that there are restrictions based on the type of backup media. The Start Time plus the duration of the archive cannot extend through midnight if archiving to a tape drive and it cannot be within the half hour preceding midnight if archiving to another disk drive.
3. Check the Day(s) of the Week on which the database backup is performed. At least one day must be checked to enable this automatic feature.
4. Specify the media on which the backup is to be performed. If the archive is coordinated with an existing tape backup program, enter the maximum duration of the backup; if archiving to another drive, enter its destination path. Check Create a sub-directory for each backup, if desired, to generate an independent folder for each backup and specify how many subdirectories are retained before they are deleted from the system. Also check to include historic data in the backup or leave the selection blank to archive only

the information logged since the previous data backup.

5. Click OK to enable the displayed **Data Backup** settings. Archiving will be performed automatically at the scheduled time on the selected day(s).

Database Server Name

Identifies the remote SQL Server where the database resides. This Server Name appears whenever it is reported, such as in Message Management, Reports and for Heartbeat functions. The Name can be a maximum of 29 characters and the field may be blank if a local SQL database engine is being used.

Data Bits

Are the number of Data bits in each transmission packet. Other values are available by pressing the associated arrow.

Days of the Week

Identifies the Days for which the displayed Availability Time entries apply.

Defaults

Restores the setting(s) to the original factory installed value(s).

Delay Alarm

When Enabled, is the period of time (in seconds) before an alarm detected on this channel is reported. The default is to report alarms immediately.

Delays

Determine how long after an alarm is reported before messaging is initiated on the *Notification List*, as well as whether this delay is observed the first time the **List** is called.

Delete Master Heartbeat Device

Removes this Server from Master Heartbeat duties.

Description

Is a user-entered comment identifying the channel.

Device Channel Count

Displays the Total number of data points on this Device tallied as Analog, Digital, Text and Time channels..

Device Description

Identifies the equipment, its current operational Status and the time of the Last Scan for data by the Foreseer Server.

Device Disabled

When checked, data are not being archived to the Foreseer Server for this Device. Disabling a Device is useful when making repairs to avoid archiving inappropriate readings.

Device Disarmed

When checked, Alarm Limit testing is suspended on all channels on this Device. Data, however, continue to be archived. Disarming a Device is useful when making repairs to avoid reporting nuisance alarms.

Directory List Box

Itemizes the files and folders within the current directory.

Disable All

Disables all optional settings for this screen.

Domain

Identifies the Domain to which the named User belongs.

Down Button

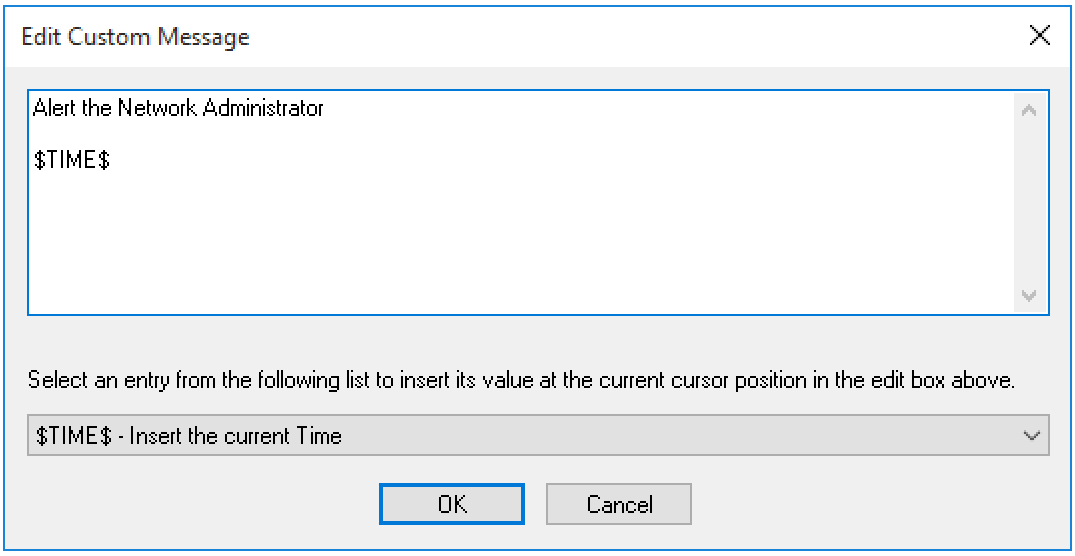
Clicking this button moves the selected person down one position in the Notification List.

Edit Button

Allows you to modify the selected item.

Edit Custom Message

The **Edit Custom Message** dialog box is reserved for sending specially formatted Alpha Paging or Command Line messages. Simply type the desired Custom Message in the text box provided. You also can Insert the Server Name, Device Name, Channel Name, Alarm Message, Current Date and/or Current Time into the text by placing the cursor in the desired location within the text box and then selecting these optional entries from the drop list below. With the Custom Message entered, click OK to save it for this channel alarm condition; Cancel deletes the Message. Note that this method requires more memory from the Foreseer application than the Standard Alarm Message format.



Edit Custom Message

Alert the Network Administrator

$TIME$

Select an entry from the following list to insert its value at the current cursor position in the edit box above.

$TIME$ - Insert the current Time

Enable

When checked, activates monitoring of a *Meters* (analog) channel's Cautionary (yellow) and Critical (**red**) Limits: a Status (digital) channel is either enabled or disabled. Alarm monitoring for all of a Meters channel's thresholds can be suspended by checking Channel Disarmed in its *General Properties* dialog box.

Enable Acknowledge Rearm

Permits a User to Acknowledge (and Rearm) alarm channels through the Web Server function. Note that this function is only available for HTTP/HTTPS Servers operating in the Text Mode.

Enable All

Enables all optional settings for this screen.

Enable Scaling

When enabled, allows you to apply a linear scaling factor to the channel's Minimum and Maximum Raw and Scaled Values. Only integer Values are acceptable entries and this settings should only be altered at the direction of Eaton personnel.

Enable the ASCII Alarm Interface

When checked, activates the Foreseer ASCII Alarm Interface function. Enabling or disabling this function requires that the computer be restarted before the state change takes effect.

Enable the HTTP Server

When checked, activates the Foreseer Web Server function. Text Mode is a text-only presentation of Server information, WebViews Mode displays Foreseer Views in the Browser similar to how they are presented on the Client. Enabling (or disabling) this function requires that the computer be restarted before the state change takes effect.

Enable the HTTPS Server

When checked, activates the Foreseer HTTP Web Server function. Text Mode is a text-only presentation of WebViews Server information, WebViews displays Foreseer WebViews in the Browser. Enabling (or disabling) this function requires that the computer be restarted before the state change takes effect.

Enable the Slave Heartbeat Function

Checked, the Heartbeat Function is activated on this Slave Server, its periodic signal sent to the displayed Master Server LAN or Dial-Up Address. Unchecked, this function is disabled.

Enable the SNMP Agent

Activates the optional Foreseer SNMP interface. This box *must* be checked for the SNMP **Virtual Agent** to work; unchecked inhibits SNMP operation.

Enable the TABS Interface

Activates this Legacy alarm interface.

Ending Date Time

The date and time at which the Custom Report terminates.

Exclude Device or Channel

Displays the *Device/Channel Selection* dialog box, allowing individual Foreseer Server Devices and/or Channels to be excluded from a Custom Report. By default, all Devices and channels are included in the report.

Exclude String

Performs a text search omitting the criteria entered in the **Custom Search** dialog box. Be sure to observe the character restrictions.

False String

Is the operational State that will be reported for this channel when its Current Value is FALSE.

File Name

Is the user-selected name of the Foreseer file.

First-Char Timeout

Is how long (in milliseconds) to wait for a response from the Device after issuing a command.

Flow Control

Determines how the data transactions are handled between the Foreseer Server and the target Device. Other selections are available by pressing the associated arrow:

Xon/Xoff - enables software handshaking between the Server and the Device.
Hardware - enables hardware handshaking between the Server and the Device.
None - no handshaking is enabled.

Foreseer Window

The **Foreseer Server** window presents the Tree View, as well as other application displays such as Meters (analog) and Status (digital) **Channel Properties** dialog boxes and the Online Help. Clicking on the right mouse button with the pointer inside the Tree View presents a context-sensitive menu.

Frequency of Calls

Specify the number of times the Notification List will be called as well as how many times each individual on the **List** will be called until a response is received. There is also a provision for specifying how many times the **List** will be recalled in the event none of the Subscribers responds to the initial notification.

Group Name

Identifies the collection of Foreseer Clients who are Authenticated access to a Web Server, as well as whether they can Acknowledge and Rearm Alarms .

Heartbeat Interval

Is the number of minutes that elapse between each issuance of the named Slave Server's Heartbeat signal. The default Heartbeat Interval is 720 minutes (12 hours), but you may wish to stagger this Interval when multiple Slaves are being monitored.

Identification Information from Device

Reflects the basic configuration parameters that the Server obtained from the equipment during Device Installation including its Address and power ratings.

Include Device or Channel

Displays the Device/Channel Selection dialog box, allowing individual Foreseer Server Devices and/or Channels to be included in a Custom History Report. By default, all Devices and channels are included in the report.

Include String

Performs a text search based on the criteria entered in the **Custom Search** dialog box. Be sure to observe the character restrictions.

Insert Channel

Displays the **Select Channel to Insert** dialog box, allowing existing inputs to be included in the Derived Channel transfer Equation.

Inter-Character Timeout

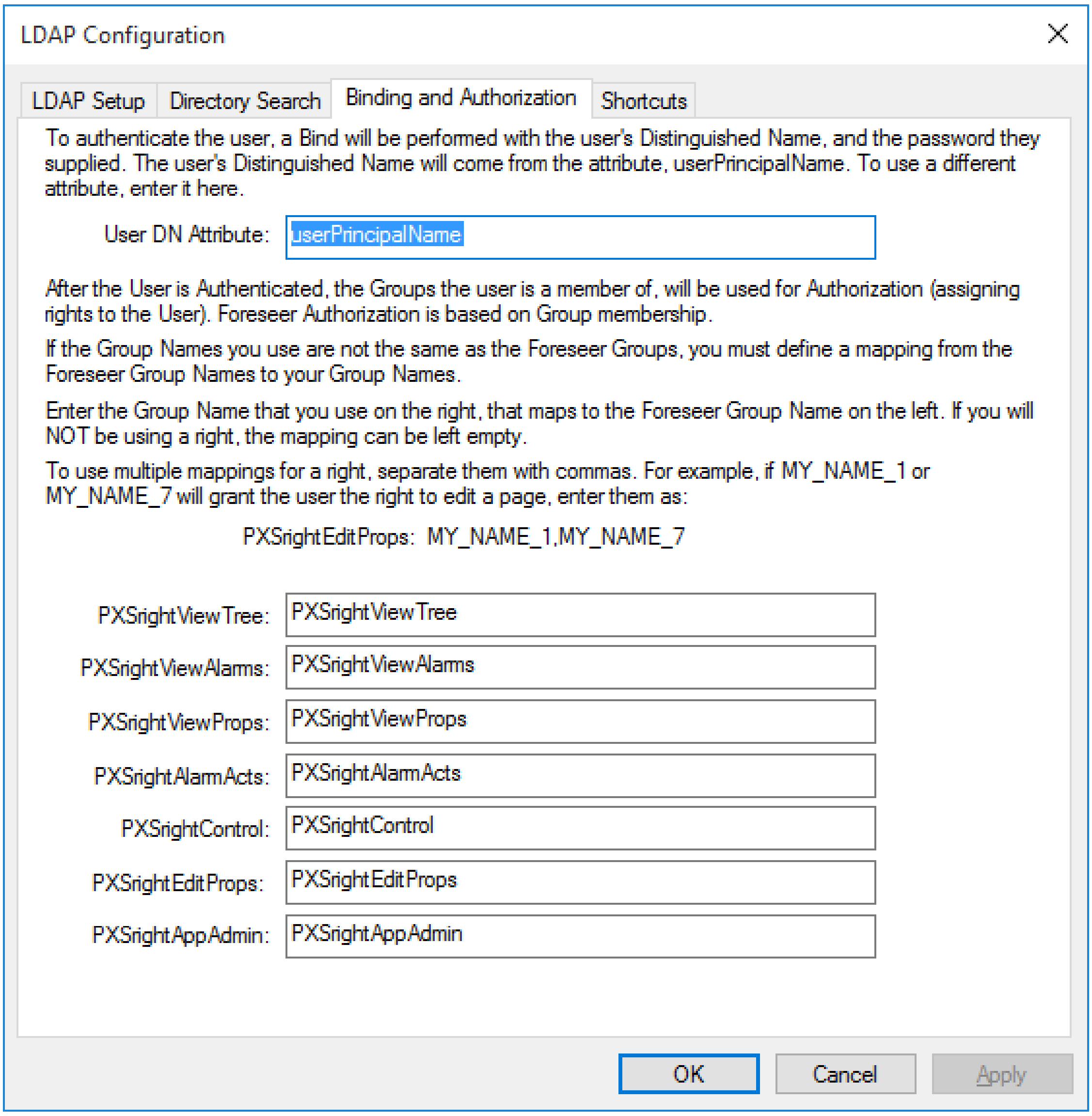
Is the period of silence (in milliseconds) to wait during a Device response before determining the message is complete.

IP Addresses

Is the list of TCP/IP Addresses for the SNMP Communities. These IP Addresses ***must be correct*** or Foreseer will be unable to establish communications with the listed host(s).

LDAP Binding

This tab associates groups to which a user belongs to Foreseer groups, granting that user rights within Foreseer. Essentially, you specify the attribute that returns the distinguished name in the user DN Attribute field and then map objects that define user groups in LDAP in the appropriate Foreseer group field. Typically, you will be matching on common name (CN) objects, as is shown in the example. If you wish to grant membership in a Foreseer group to multiple LDAP user groups, separate these object definitions with a comma. For more about Foreseer groups, see the *Foreseer Server Guide*.



To authenticate the user, a Bind will be performed with the user's Distinguished Name, and the password they supplied. The user's Distinguished Name will come from the attribute, userPrincipalName. To use a different attribute, enter it here.

User DN Attribute: userPrincipalName

After the User is Authenticated, the Groups the user is a member of, will be used for Authorization (assigning rights to the User). Foreseer Authorization is based on Group membership.

If the Group Names you use are not the same as the Foreseer Groups, you must define a mapping from the Foreseer Group Names to your Group Names.

Enter the Group Name that you use on the right, that maps to the Foreseer Group Name on the left. If you will NOT be using a right, the mapping can be left empty.

To use multiple mappings for a right, separate them with commas. For example, if MY_NAME_1 or MY_NAME_7 will grant the user the right to edit a page, enter them as:

PXSrightEditProps: MY_NAME_1,MY_NAME_7

PXSrightViewTree: PXSrightViewTree

PXSrightViewAlarms: PXSrightViewAlarms

PXSrightViewProps: PXSrightViewProps

PXSrightAlarmActs: PXSrightAlarmActs

PXSrightControl: PXSrightControl

PXSrightEditProps: PXSrightEditProps

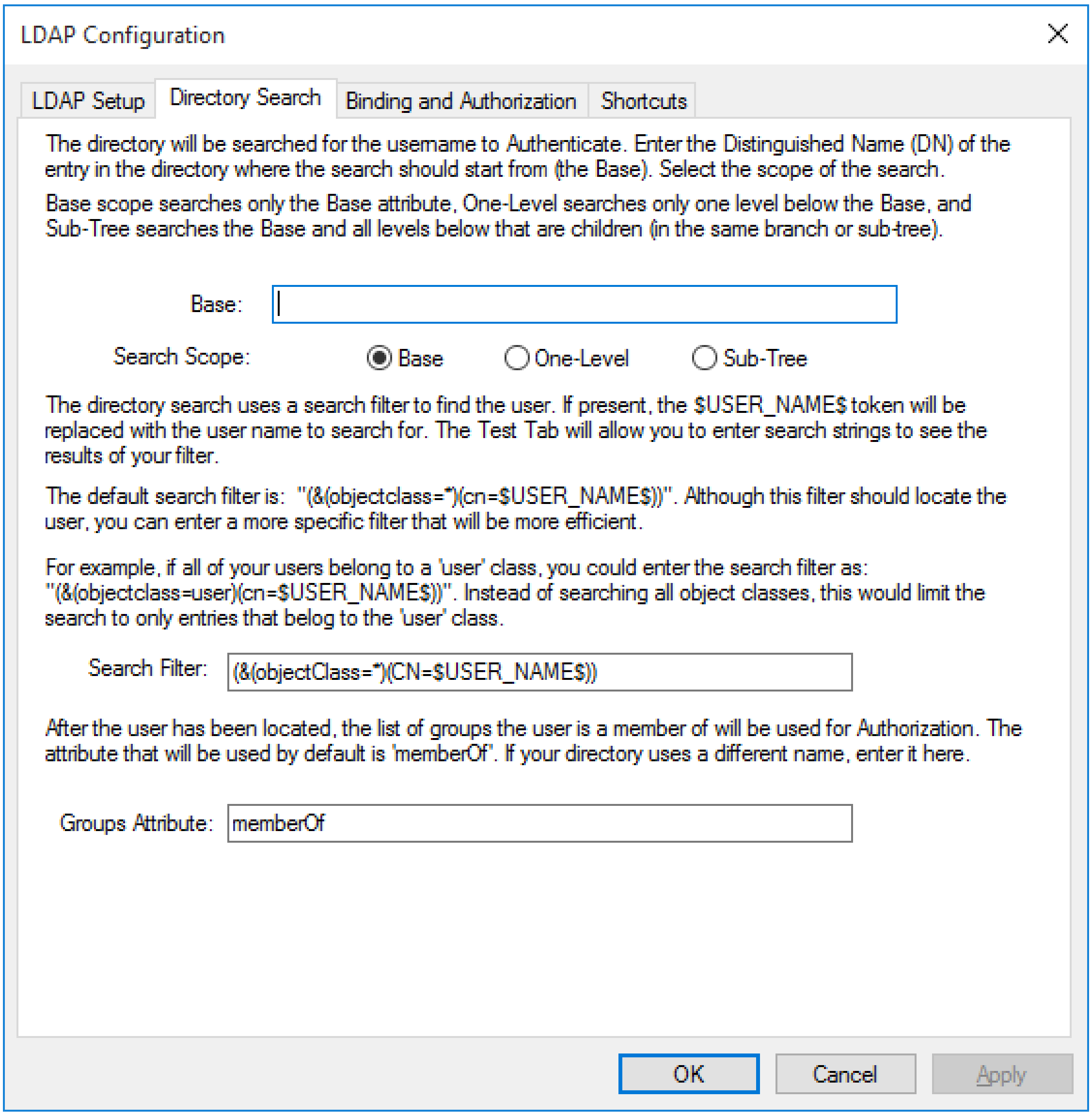
PXSrightAppAdmin: PXSrightAppAdmin

LDAP Directory

You must set the base distinguished name (dn) that Foreseer will use to run queries on the directory server. The subtree search starts from this distinguished name. You must also set the query depth (Search Scope).

The filter that is preloaded in the Search Filter was designed to find user objects in most situations. However, you can enter your own string tailored to your system. The example shown in the following figure has such a string.

The final field specifies the attribute that will return all groups to which a user belongs. If you use a different attribute you'll need to replace the default string.



The directory will be searched for the username to Authenticate. Enter the Distinguished Name (DN) of the entry in the directory where the search should start from (the Base). Select the scope of the search.

Base scope searches only the Base attribute, One-Level searches only one level below the Base, and Sub-Tree searches the Base and all levels below that are children (in the same branch or sub-tree).

Base:

Search Scope: ● Base ○ One-Level ○ Sub-Tree

The directory search uses a search filter to find the user. If present, the $USER_NAME$ token will be replaced with the user name to search for. The Test Tab will allow you to enter search strings to see the results of your filter.

The default search filter is: "(&(objectclass=*)(cn=$USER_NAME$))". Although this filter should locate the user, you can enter a more specific filter that will be more efficient.

For example, if all of your users belong to a 'user' class, you could enter the search filter as: "(&(objectclass=user)(cn=$USER_NAME$))". Instead of searching all object classes, this would limit the search to only entries that belog to the 'user' class.

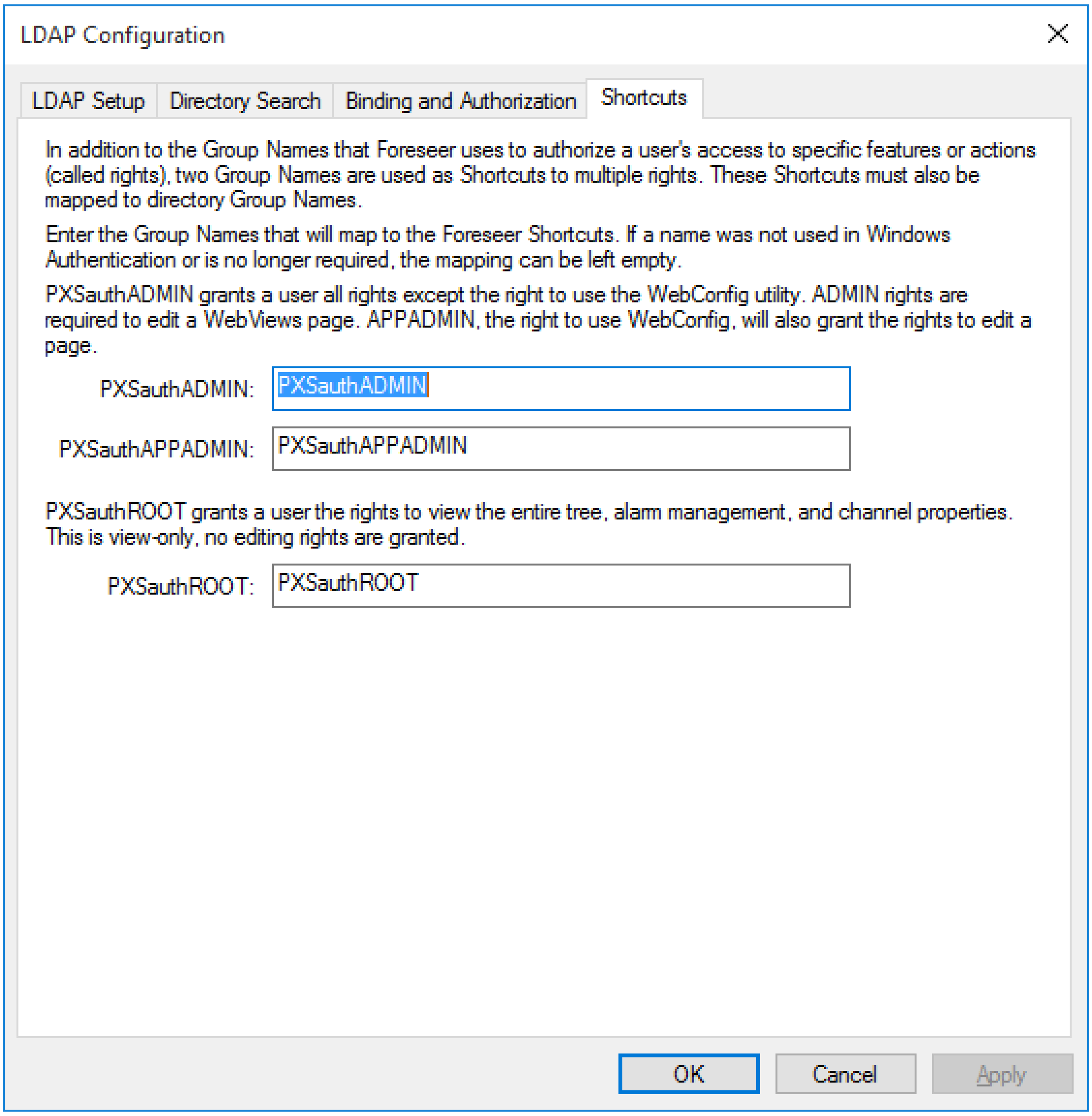
Search Filter: (&(objectClass=*)(CN=$USER_NAME$))

After the user has been located, the list of groups the user is a member of will be used for Authorization. The attribute that will be used by default is 'memberOf'. If your directory uses a different name, enter it here.

Groups Attribute: memberOf

LDAP Shortcuts

Foreseer has two "superuser" groups: PXSauthADMIN and PXSauthROOT. You can also map these to LDAP user groups. For more about Foreseer user groups, see the *Foreseer Server Guide*.



In addition to the Group Names that Foreseer uses to authorize a user's access to specific features or actions (called rights), two Group Names are used as Shortcuts to multiple rights. These Shortcuts must also be mapped to directory Group Names.

Enter the Group Names that will map to the Foreseer Shortcuts. If a name was not used in Windows Authentication or is no longer required, the mapping can be left empty.

PXSauthADMIN grants a user all rights except the right to use the WebConfig utility. ADMIN rights are required to edit a WebViews page. APPADMIN, the right to use WebConfig, will also grant the rights to edit a page.

PXSauthADMIN: PXSauthADMIN

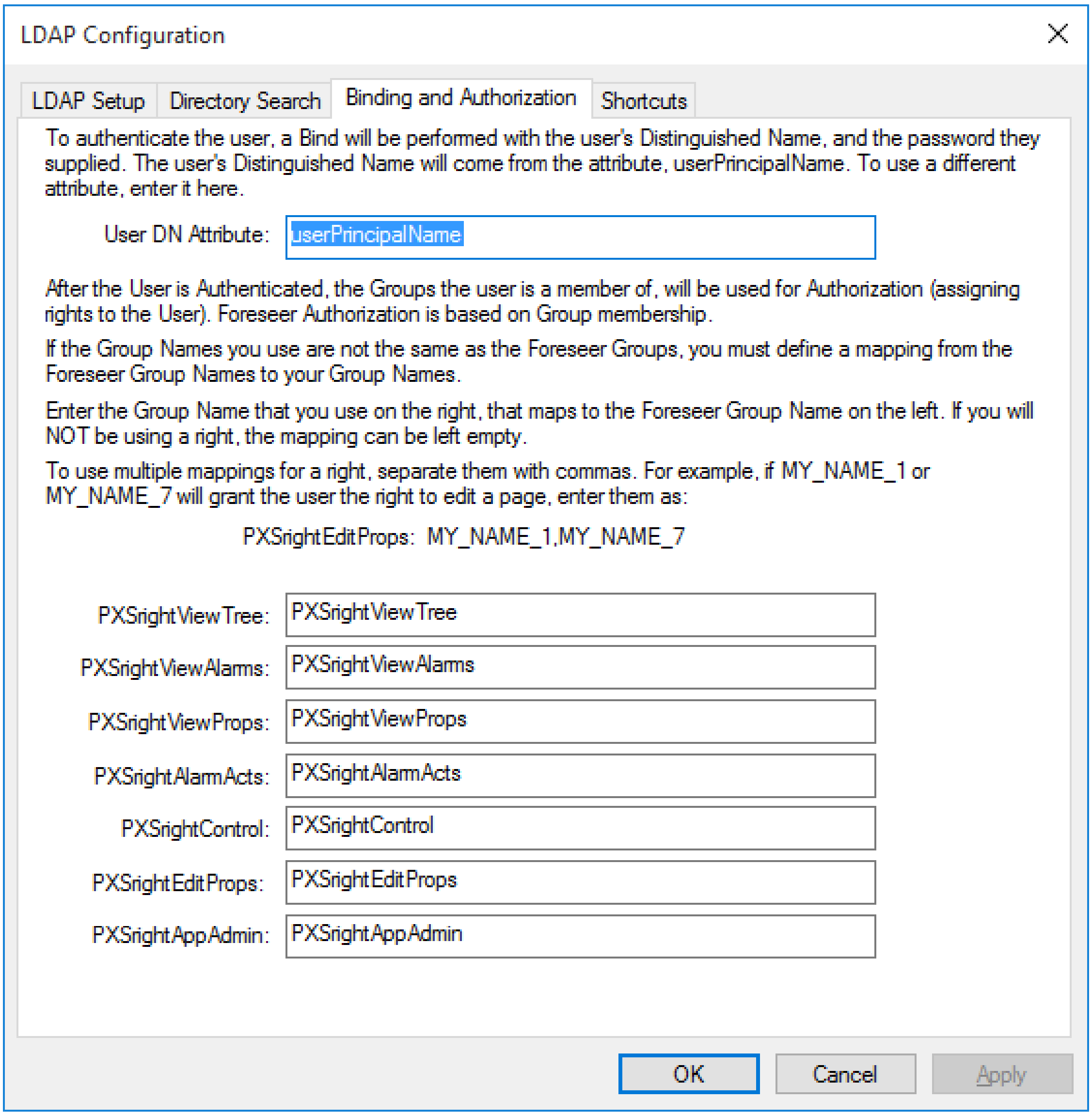
PXSauthAPPADMIN: PXSauthAPPADMIN

PXSauthROOT grants a user the rights to view the entire tree, alarm management, and channel properties. This is view-only, no editing rights are granted.

PXSauthROOT: PXSauthROOT

LDAP Testing

You can test an individual LDAP account to see what Foreseer groups are mapped to it. This is extremely useful in verifying that all of the settings are correct.



To authenticate the user, a Bind will be performed with the user's Distinguished Name, and the password they supplied. The user's Distinguished Name will come from the attribute, userPrincipalName. To use a different attribute, enter it here.

User DN Attribute: userPrincipalName

After the User is Authenticated, the Groups the user is a member of, will be used for Authorization (assigning rights to the User). Foreseer Authorization is based on Group membership.

If the Group Names you use are not the same as the Foreseer Groups, you must define a mapping from the Foreseer Group Names to your Group Names.

Enter the Group Name that you use on the right, that maps to the Foreseer Group Name on the left. If you will NOT be using a right, the mapping can be left empty.

To use multiple mappings for a right, separate them with commas. For example, if MY_NAME_1 or MY_NAME_7 will grant the user the right to edit a page, enter them as:

PXSrightEditProps: MY_NAME_1,MY_NAME_7

PXSrightViewTree: PXSrightViewTree

PXSrightViewAlarms: PXSrightViewAlarms

PXSrightViewProps: PXSrightViewProps

PXSrightAlarmActs: PXSrightAlarmActs

PXSrightControl: PXSrightControl

PXSrightEditProps: PXSrightEditProps

PXSrightAppAdmin: PXSrightAppAdmin

Limits

When Enabled, are the channel's monitored Cautionary (yellow) and Critical (**red**) Alarm Limits. Independent Hi and Lo Limits can be set for both event levels.

List Details

Toggles the current Windows directory display between an alphabetical listing of its files and one which also furnishes each file's Size, Type and the date it was last Modified.

Location

Is the location of the Foreseer Client equipped with the SNMP interface.

Log Messages

Reports the number of Messages that can be logged for this Device.

Look In

Is the Windows directory in which the desiredFile name is found.

Master Server Dial-Up Address

The secondary Address of the Master Server to which this Slave Server sends its Heartbeat signal. This IP (Internet Protocol) Dial-Up Networking Address is only used if the primary LAN Address connection fails.

Master Server LAN Address

The Local Area Network Address of the Master Server to which this Slave Server sends its Heartbeat signal. This IP (Internet Protocol) Address assumes the Master and Slave Servers exist on the same network. If this connection fails, the signal is sent via the secondary Dial-Up Networking.

Max Number of Connections

Limits the number of simultaneous active Browser connections permitted on the Server. Enter the desired number of allowable connections, bearing in mind that more connections will reduce the Server's response time for each request.

Max Number of Requests

Defines the data request limit for Web Browsers that support the Keep-Alive function, which maintains connection with the Web Server unless the specified Timeout period expires. Set the Max Number of Requests to "1" to disable this function.

Messages

Provides for a user-entered message to be assigned to an alarm notification sent via an alpha/numeric pager. The message must conform to the Service provider's character limitations. Optionally, the appropriateAlarm Message, entered in the errant channel's Meters or Status **Basic Properties** dialog box, can be included in the outgoing Alpha/Numeric message. When defining a channel's Messaging Properties, its Server, Device and Channel name also may be included in the message.

Messages Menu

The **Messages** menu is displayed when the **Message Management** window is active and allows you to control the notification process when an alarm is reported. Several of the commands are duplicated in the context-sensitive menu that is accessed by selecting a Message in the window's Status Display and right-clicking.

The **Messages** menu offers the following Foreseer commands:

> ✓ Any grayed commands are unavailable and Administrative Authorization is required to perform **Message Management** functions.

Save Message File - Saves the contents of the **Message Management** window (excluding the information in the Status portion) to a file.

Stop Call - Terminates calling the Source(s) currently highlighted in the **Status** area of the **Message Management** window.

Call Again - Re-initiates calling to the Source(s) currently highlighted in the **Status** area of the **Message Management** window.

Remove Call - Removes calling to the Source(s) currently highlighted in the **Status** area of the **Message Management** window.

Stop All Calls - Terminates calling to all Sources currently listed in the **Status** area of the **Message Management** window.

Remove All Completed Calls -Deletes all completed calls that are currently listed in the **Status** area of the **Message Management** window.

Suspend All Calls - Postpones calling to all current and pending Sources listed in the **Status** area of the **Message Management** window for one hour.

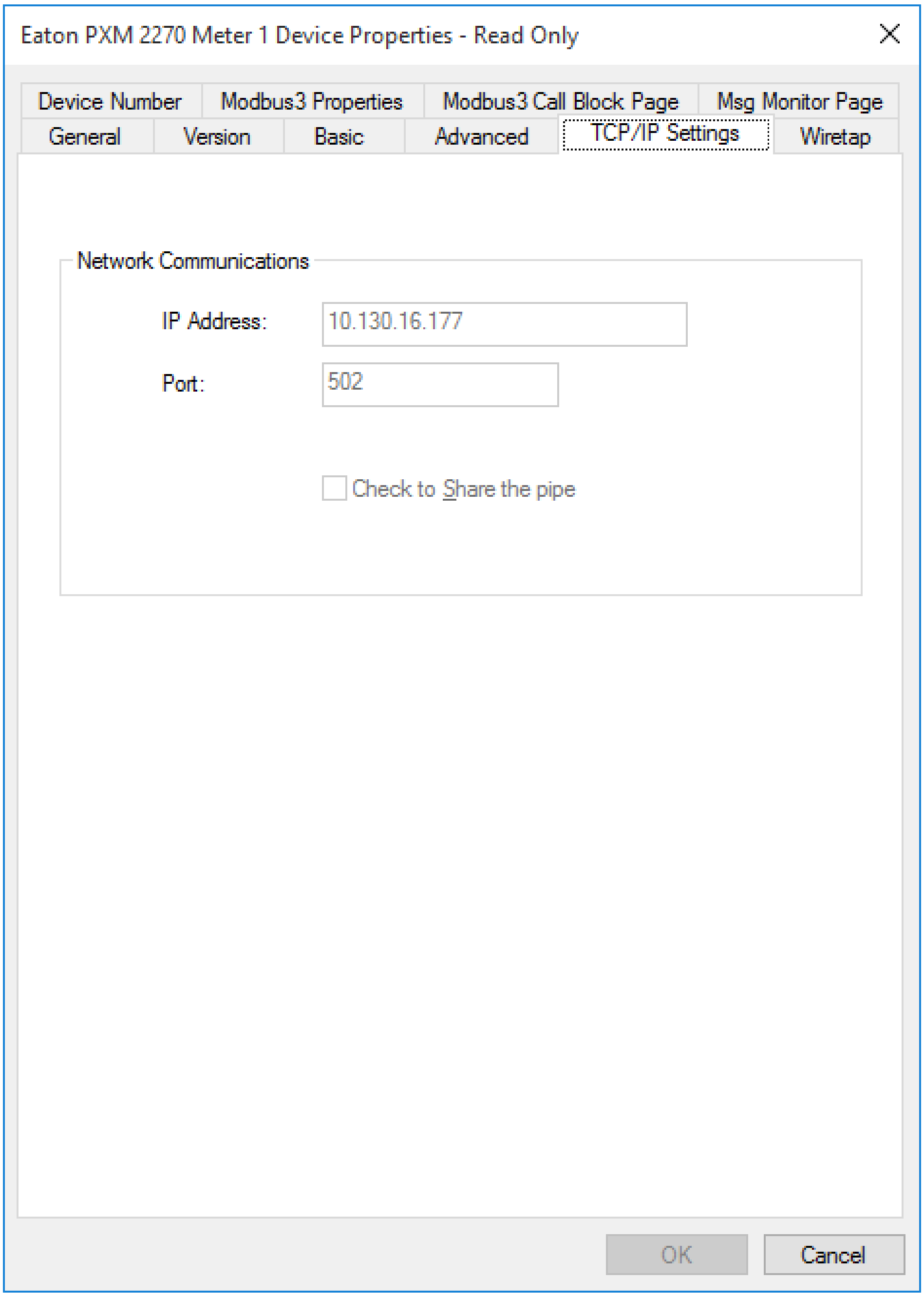
Status Messages... - Displays the Status Messages dialog box containing detailed call information on the selected Source(s).

Show Title Tips - When enabled, displays the complete message for the selected Source(s) in a pop-up tip window whenever the pointer is held over itsStatus field.

Properties - Displays the Message Properties dialog box, permitting the period for which completed messages are retained and the duration for which pending calls are suspended to be specified.

Network Connection

The Device's IP Address must be entered when utilizing a ConnectUPS Network Adapter a **Network Device Connection** during Device Installation. Obtaining this Address is the responsibility of the user and it must be correct or the Server will be unable to communicate with the target Device. With the correct Device IP Address entered, click Next > to return to the **Device Installation Wizard**.



Eaton PXM 2270 Meter 1 Device Properties - Read Only

Network Communications

IP Address: 10.130.16.177

Port: 502

□ Check to Share the pipe

New Password

Is the new Client Password required to access this Foreseer Server You must repeat the entry in the Confirm New Password field to activate it.

Notification List

Identifies the personnel to be alerted to an alarm condition on this channel by Foreseer Message Management. An existing Notification List is selected from the drop list that is displayed by clicking on the associated arrow. You may optionally specify that Foreseer Always notify regardless of Client connections by checking that box to ensure that the proper personnel are appraised.

> ✓ If upgrading an earlier version of Foreseer, any previous channel with an assigned Notification List will use it for reporting **Critical** and **Cautionary** alarm states. **Acknowledged** and **Normal** state conditions are not assigned Channel Messages by default; they must be entered manually by the User

Notification List Name

Identifies the Notification List that is used to initiate alarm messaging.

Numeric Page

Allows you to Enter the numeric message that is to be sent with the alert issued when an alarm is reported on this channel.

Parity

Is the Parity (Odd, Even, None, Mark or Space) of the transmission. Other selections are available by pressing the associated arrow.

Password

Is the current User's *Administrative Authorization*; asterisks are displayed to maintain system security. The Foreseer Web Server function offers optional security by requiring a Password to view information, generate **Reports** and Acknowledge alarms.

> ✓ Passwords are case-sensitive; therefore "USER," "User" and "user" are all recognized as different Passwords.

Port

Identify how the Device or modem is connected to the Foreseer Server. The possible Device connections are a Network or a Serial Communications interface.

Port to Listen on for HTTP

Is the port the Server will monitor for HTTP requests from Foreseer Clients. The default setting of "80" is the standard port and should not have to be changed under normal conditions.

Port to Listen on for HTTPS

Is the port the Server will monitor for HTTPS requests from Foreseer Clients. The default setting of "443" is the standard port and should not have to be changed under normal conditions.

Postfix Phone Number

Specifies any number(s) to be dialed following the the Service Number, such as a Password.

Pre-defined Time Interval Report

Allows the Custom Alarm, Audit and Notes History Reports to be run over a fixed period of time. Choose the desired Time Interval from the selections available when you click on the associated arrow.

Printer

Identifies the active printer and its connection: Click on Properties to change the printer setup. When specifying a **Printer Service**, you can only select from the drop list of Printers previously installed.

Printing Properties

Specify how the Alarm Message (up to 8 lines of text) is output by the Printer:

Prefix each message with Date and Time appends a time stamp to the beginning of the Alarm Message.
Print page after each message and Print page when messages fill printed page control

whether each Alarm Message is output individually.
Number of lines to space after each message allows you to specify a number blank lines to be inserted between Alarm Messages when they are printed on the same page.

Priority

Is a number from 1 (highest) to 9999 (lowest) which assigns a level of importance to an alarm detected on this channel.

Re-arm

Is the period of time (in minutes) before alarm monitoring is automatically restored to a disarmed channel. Rearming manually resumes testing of a channel's acquired Current Value against its specified Alarm Limits. Check the box preceding this field to Enable the setting.

Redundant Server

Specifies whether the Server is part of a redundant backup system. A Primary Redundant Server synchronizes timing between all Secondary Redundant Severs. Only one Server can be designated as the Primary Redundant or timing problems will result when adding new Servers and Devices to the configuration. If the Server is not part of a redundant system, select Stand-Alone.

Refresh Interval

Is the period, in seconds, before Web Browsers update the information in the Server screen display. This is a global setting for all Browsers that are capable of automatically refreshing their display; a setting of "0" disables this function.

Remove Slave

Deletes the identified Slave Server Name in the associated list box for Heartbeat function.

Report Interval

Is the calculated span of the Custom Report based on the Starting and Ending Date/Time entries.

Resend Interval

Is the delay (in minutes) before a trap is resent. One of the Resend Options must be enabled to select this feature.

Resend Options

Allows you to resend traps forall alarms or only unacknowledged alarms once the delay specified in the Resend Interval has expired, or disable the **Resend Traps** feature completely.

Restore Defaults

Loads the default Windows **Control Panel /** COM Port settings.

Retry Time

Is the delay between attempts to reconnect to a disconnected SQL Server. The default Retry Time is 30 seconds: A setting of "0" seconds disables this feature until a new setting is entered.

Scan Interval

Is the delay (in milliseconds) between data polls of the Device.

Scan Time Watchdog

Monitors the Scan Interval for the Device. Assuming it is enabled and does is not reporting a communications alarm, a system error will be generated if the period between successful scans of the Device exceeds the specified Watchdog Time interval.

Secondary Data Path

Applies only to Jet databases and may be entered to designate an alternate location where Foreseer attempts to retrieve historical data when the requested information is not located in the active data directory. (The use of Jet is deprecated.) Typically, this is a larger hard drive located on the network that can provide the significant storage capacity required for the high-resolution data accumulated over time. The secondary location can be specified as the **Database.** *Backup Path*, if desired. You also can Browse... the network to locate the desired destination.

Separator Character

Separates the text between individual ASCII alarm outputs.

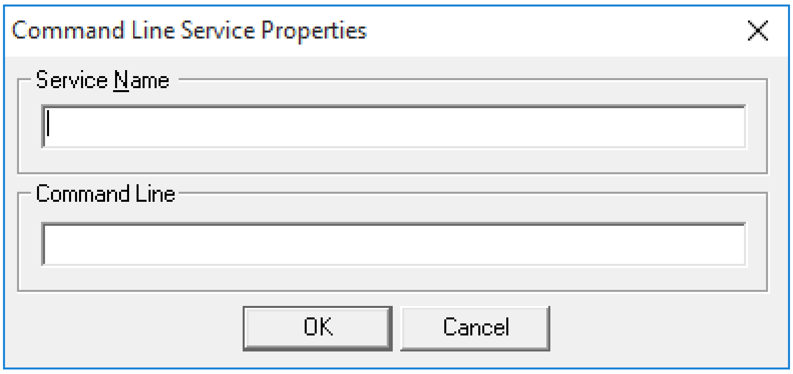
Service Name

Identifies the Service that is used to initiate the alarm notification or command.

Service Properties - Command Line

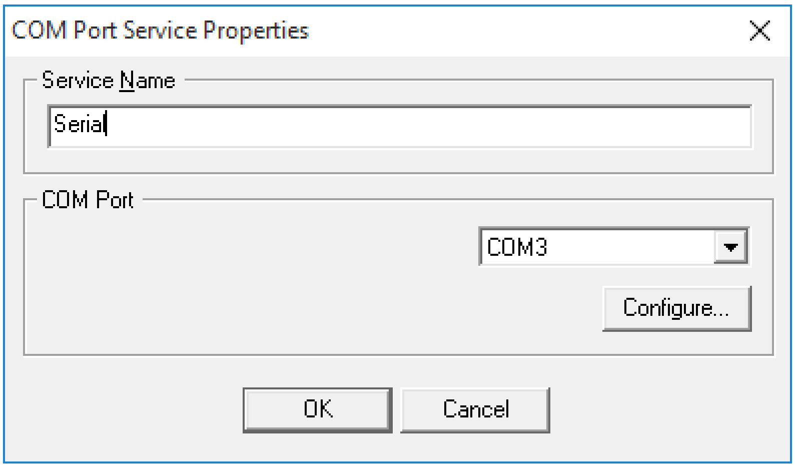
The **Command Line Service Properties** dialog box is used to configure a custom Message Management **Service**. It can be used to issue a notification via a Service which is not already defined through one of the existing out call options, or the command could launch another application. If a Command Line entry is made here, it is applied globally to all alarm channels subscribing to this **Service**. Specific Command Line instructions can be applied to individual channels using Foreseer Channel Message Settings.

✓ If you intend to create Custom Messages for individual channels, leave the Command Line field blank.



Service Properties - Output to COM Port

The **COM Port Service Properties** dialog box is used to configure the parameters for that particular type of messaging *Service*. Clicking in a field below displays its function.


COM Port Service Properties

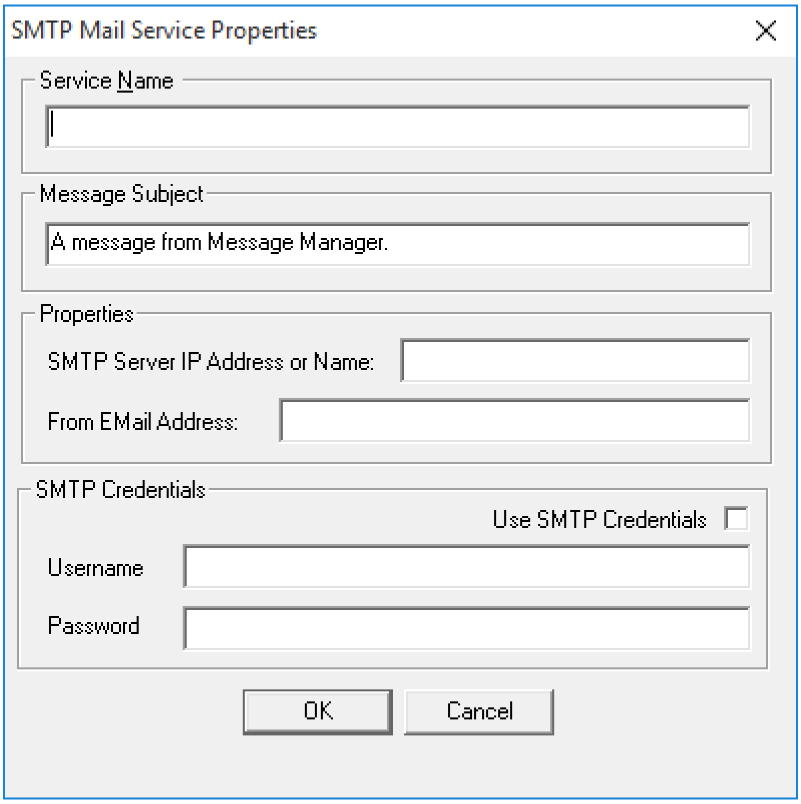
Service Name: Serial

COM Port: COM3

Service Properties - SMTP Mail

The **SMTP Mail Service Properties** dialog box is used to configure the parameters for Simple Mail Transfer Protocol messaging. An SMTP Server is required for this *Service* to be available to Foreseer.

In addition to specifying an email address and SMTP server, you can also specify a User-name and Password for the account.


SMTP Mail Service Properties

Service Name:

Message Subject: A message from Message Manager.

Properties

SMTP Server IP Address or Name:

From EMail Address:

SMTP Credentials

Use SMTP Credentials □

Username

Password

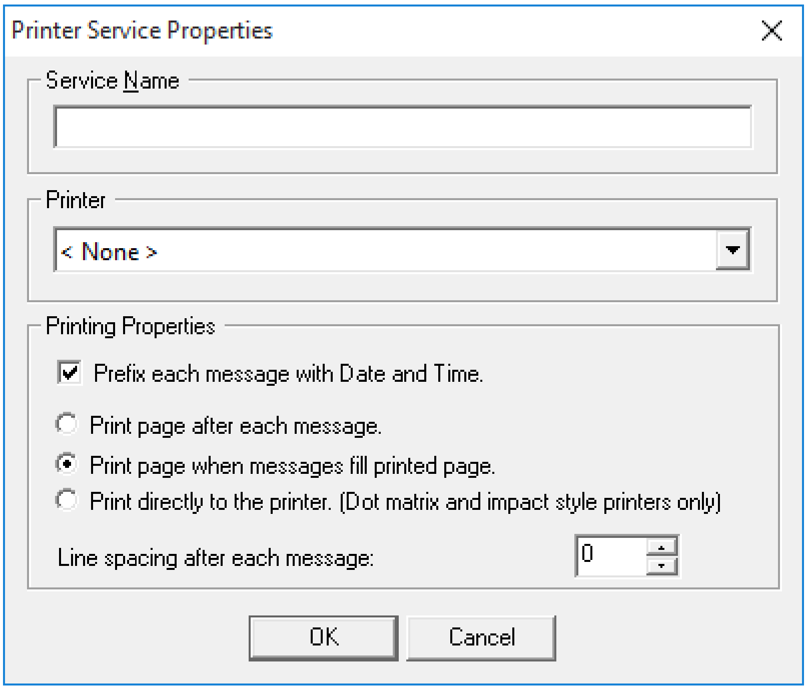
Settings Button

Allows the serial interface settings to be specified for the named Port through the *COM*

Properties dialog box.

Service Properties - Printer

The **Printer Service Properties** dialog box is used to configure the parameters for that particular type of messaging *Service*. Clicking in a field below displays its function.



Printer Service Properties

Service Name

Printer: < None >

Printing Properties

☑ Prefix each message with Date and Time.

○ Print page after each message.

● Print page when messages fill printed page.

○ Print directly to the printer. (Dot matrix and impact style printers only)

Line spacing after each message: 0

Significant Characters for Location Names

Specifies the number of significant characters identifying the alarm location.

Slave Server Name

Identifies the Slave Server to the Master Heartbeat Server. The Name shown must match the one that appears in the Slave Server's *Properties* dialog box *exactly* or the two computers will not communicate properly.

SMTP Server IP Address or Name

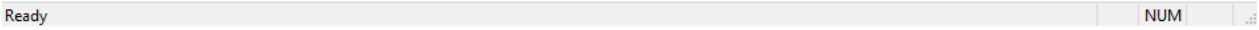
Is the Internet Protocol Address or Name of a Simple Mail Transfer Protocol Server.

Sound Horn

Alerts personnel via an audible signal whenever a specified alarm state is detected. These conditions--Critical (**Red**), Cautionary (**Yellow**) Acknowledge (**Blue**)--are enabled by checking the appropriate box(es).

Status Bar

The **Status Bar** displays context-sensitive messages which aid program activity, such as the operation resulting from selecting a particular menu command. The right side of the **Status Bar** shows when the Caps Lock (CAP), Numeric Lock (NUM) and Scroll Lock (SCRL) keys are active. The **Status Bar** itself can be hidden and displayed (default) by toggling the Status Bar command in the Windows menu; a check preceding the command indicates when it is enabled.



Status Messages

Displays the Status Messages dialog box containing detailed call information on the selected Source(s).

Stop All Calls

Terminates calling to all Sources currently listed in the **Status** area of the *Message Management* window.

Stop Bits

Are the number of Stop bits in the transmission. Other selections are available by pressing the associated arrow.

Stop Call

Terminates notification to the Source(s) currently selected in the **Status** area of the *Message Management* window.

Subscriber Name

Identifies the individual to whom the **Properties** apply.

Suspend All Calls

Postpones calling to all current and pending Sources listed in the **Status** area of the **Message Management** window for the period specified in the **Message Properties** dialog box.

Synchronize Remote's Clock on Connect

Automatically updates the current time on the Remote Server on connection.

TCP Port

Is the port through which the ASCII text alarm is output.

Temporarily Disable the Connection Retry

Allows you to temporarily disable the automatic retry connection feature when maintenance or other procedures are being performed on the SQL database Server. This setting can be unchecked manually to restore automatic reconnection, or is automatically reset when the local Server PC is rebooted.

Terminal Server Connection

When checked, indicates the Device is physically attached to a Terminal Server.

Test Button

Simulates an input to the displayed Equation and reports the result in the associated Channel field. Testing the Equation permits its operation to be verified before the channel is placed into service.

Test Call Button

Verifies proper operation of the selected call. The *Call Now* dialog box is displayed, allowing you to enter Alpha and/or Numeric Messages to be sent, as well as assign them Primary and Secondary Priorities. Click OK and the progress of the Test Call is reported in the Status portion of the **Message Management** window.

Timeout

Is the interval of inactivity (in seconds) before connections are terminated. The Timeout period applies to update Requests in Web Browsers that support the Keep-Alive Function as well as the ASCII Alarm Interface.

Title Bar

The ***Title Bar*** identifies the Foreseer application and the active window. Minimize, Maximize and Close, are standard Windows buttons which perform those program functions. These three operations are also available as commands, along with Windows Restore, Move and Size functions, by left-clicking on the Foreseer Server icon or right-clicking on the ***Title Bar*** itself.

True String

Is the operational State that will be reported for this channel when its Current Value is TRUE.

Unavailable

If checked, inhibits paging of this Person within any Notification List to which he or she belongs.

Units

Are the measurement units in which the channel's data are reported.

Up Button

Clicking this button moves the selected person up one position in the *Notification List*.

Up One Level

Moves the active directory up one level in the Windows hierarchy.

User Name

Identifies the current Foreseer User.

Value

Is the date and time a Date Channel state is True, triggering an alarm condition.

Verify Password

Is a security feature that requires a New Password be entered a second time in order to confirm changing it.

View Menu

The **View** menu allows the Foreseer Server display (primarily the *Tree View*) to be customized. The commands are much like those used in Windows Explorer.

You can enable/disable the Tool bar and / or Status Bar, adjust the Split bar between the left and right window panes and format the information displayed in the right pane as Small Icons, a List or show the Details for each item. All currently open Views also are listed, a check preceding the active display.

The **View** menu offers the following Foreseer commands:

Status Bar - when checked, enables the Foreseer Server *Status bar*.

Split - automatically selects the Windows splitter for a *Tree View*, allowing the relative size of the window pane displays to be changed.

List - when checked, displays the icons in right pane of the *Tree View* as a continuous alphabetical list.

Details - when checked, shows detailed information about the component selected in left pane of the *Tree View* on the right side of the display.

WebViews

WebViews represent the latest generation of Foreseer enterprise monitoring. The WebViews web editor is not a fully functional web interface, nor is it a drawing and design tool. Rather it is a bridge between server programing and graphic user interface design. WebViews allows you to custom design all aspects of your site through an extensive collection of drawing tools and view it through Microsoft Internet Explorer.

WebViews allows you to create as much complexity as you like without learning the intricacies of web design. The first thing to remember when starting any project is to plan. The more planning you do initially, the less trouble you will encounter during the course of the project.

Creating WebViews Folders

You can create WebViews folders and populate these with devices and channels. The following details the functions in the WebViews right-click menu.

New Folder

Creates a new folder as a child of the currently selected folder. The corresponding WebViews page is also created.

Delete

Deletes the currently selected folder and WebViews page.

Cut

Cuts the currently selected folder (and WebViews page) so that it can be pasted to another location in the tree. There's no visual indication that the folder has been cut; however, following a Paste operation its location in the tree will change.

Copy

Copies the current folder and pastes the copy as a child of the selected folder.

Copy Link

Copies a link to the selected folder, which when pasted provides a link to that folder instead of a copy. The link has the path to the target folder in its name and is shown with a blue folder icon.

Pastes the result of a Cut, Copy, or Copy Link operation as the child of the selected folder.

Create a Single Page/Create Pages for Tree

Recreates the WebViews page files for the selected folder in the tree. Two files, index.htm and layout.xml, are created when a WebViews Folder is created (they reside in the \Program Files (x86)\Eaton Corporation\Foreseer\WWW\WebViews folder on the server machine in a tree that mimics the structure of the WebViews tree. Should you corrupt either of these files in the course of editing (especially by editing the files directly), you can delete them and use this command to regenerate new files based on the system defaults.

The Create Pages for Tree function will recreate pages as needed for the selected folder and its children. New pages will be recreated only if either of the files for that folder are missing.

Templates

Templates provide a way to build WebViews pages quickly by using one page as a model for others. The Templates menu provides the following functions:

Create Page from Template/Create Tree from Templates

To create a WebViews page or tree section from a template file:

1. Creates a WebViews page or a section of the WebViews tree from the specified Template file. The page(s) can include specified Devices and their Channels.
2. Right-click the location for the page in the WebViews tree and select Templates → Create Page from Template.
3. Select the .tpf template file to use. Template files for the currently selected folder in the templates tree are in the right pane. You can navigate through the tree (left pane) to select files in other locations in the tree.
4. Click Open.
5. Select Use the same objects that are in the template to link to these objects automatically (if they are still available on the server). Selecting this option pre-populates the Device to Use field in the next dialog box. If you wish to select another device at that point, you still can even if this option is selected.
6. In this step, you must select the device in the template and match that to an existing device in the server. The Device to Use field shows the currently selected device. You can select the server in the left pane and any device on the right pane. If you do not select a device identical to what was in the template, objects in the WebViews page will not have matching Channels and must be manually relinked.
7. When you've selected a device, click Create.

Create Single Template/Create Templates for Tree

If you're using Create Single Template the resulting template file is based on the selected WebViews page. This file will can then be used to create a copy of this WebViews page at different locations in the tree. If you're using Create Templates for Tree, the resulting template file can be used to create a copy of the selected WebViews page and all of its children. You can use this function to rapidly recreate repeating tree structures throughout the WebViews tree. For both functions, you can specify the device to use when specifying attached channels.

To create a template file:

1. Right-click a folder in the WebViews tree and select Templates → Create Single Template or Templates → Create Templates for the Tree. If you are using the Create Templates for Tree function, all of the child folders will also be included in the template file.
2. Select a location in the Web Templates tree and specify a file name for the .tpf template file. You can use the New Folder button to create a new folder as a child of the folder currently selected in the Web Templates tree. This simply creates a folder in the Foreseer Server file system (under \Program Files (x86)\Eaton Corporation\Foreseer\Web Templates).
3. Click Save.
4. Check files for Page
5. This function is for specialized applications, and should only be used at the direction of Eaton technical support.
6. Check Files for Tree

Channel Configuration

You can delete a channel from a selected folder in the WebViews tree.

To delete a channel from a WebViews folder:

1. Select a folder in the WebViews tree.
2. In the right pane, select one or more channels. You can use Shift-click to select a range of channels and Ctrl-click to multi-select channels.
3. Right-click over one of the selected channels and choose Delete.

Design Considerations

The Foreseer editor is relatively simple to learn. A user with a basic background in web design and image creation software should be proficient on the software in less than a day. Keep in mind that you can create many of the assets that you need inside the WebViews, but some elements such as .jpg, .gif, .png, and flash components require additional software to create.

When beginning a WebViews design, it is important to know what you want to create: what equipment drivers and channels you will have to add to the Server so you have the correct data in place; and what folder structure you will have to create on the for a logical separation of data. Keep in mind that if you are going to create templates from the page, you must plan for future expansion and include the largest number of channels and other objects that will ever be placed in the pages. Any pages that you create based on the template that have less than the maximum amount of data can have extraneous channels and objects deleted. By incorporating the maximum number of potential objects at the outset, you can anticipate potential problems and change the design as necessary rather than reworking it later.

Page Layout

The WebView Editor is a web layout program designed to allow users the ability to create data interfaces with little or no knowledge of web software. However, as with any layout, it is important to plan ahead and simplify the structure of the page to consider future maintenance. The best way to get started is with a pencil and paper. Initially, block out areas for object placement using squares with general text descriptions to identify the objects that will fill the space. Once you have the basic layout for the page, decide which objects should be grouped for easy editing. You may want to group objects like images together, or place all the user interface objects in one layer group. It is not important that you get the layout exactly right because as the project progresses changes inevitably will be made. But if you get the basic elements in place, future changes are much less time-consuming.

Remember that the WebView Editor is not a drawing program, so you can not create vector or raster art. You are also limited by the web browser paradigm. In other words, line objects created in the editor may be square, horizontal or vertical, but curves, diagonals or rounded corners can only be introduced by placed image objects.

Layer Groups

It is very important to plan layers for your pages. Because you may be adding many elements to a page, including some that overlap, you will want an easy way to select objects. One of the features of the WebViews Editor are the Layer Groups, which allow you to turn the editing capabilities of any object that exists in a specific Layer Group on and off. To take full advantage of this capability, you must plan which objects are going to be at the lowest Z-index and which are going to be at the highest Z-index(Z-index is a DHTML value that places an object nearer or farther from a view based on an assigned number). The WebViews Editor has eight predefined layer groups.

Using layer groups for similar objects will speed up editing and revisions. Each "layer" consists of ten Z-index levels. Objects may be positioned inside an editable layer group and still not be individually editable using theEdit Layer command. The added Z-index levels inside the layer groups allow the user to move objects forward and backward in space. This is very important when creating complex interfaces with many overlapping objects. You can have objects positioned on Z-index "10" and Z-index "19," but both are editable when you are editing Layer "1." Be sure to isolate objects that may be difficult to select into separate layer groups once the layout is complete. This will provide the designer with maximum selection flexibility.

The following are the default Z-index settings of objects newly inserted into a WebViews page:

Layer 1	Z-index "10-19"
Layer 2	Z-index "20-29"
Layer 3	Z-index "30-39"
Layer 4	Z-index "40-49"
Layer 5	Z-index "50-59"
layer 6	Z-index "60-69"
Layer 7	Z-index "70-79"
Layer 8	Z-index "80-89"

The default Z-index can be changed by selecting the object, double-clicking and altering the Z-index field in the **Properties** dialog box to reflect the appropriate level. The level can also be changed by using the Alt+1-Alt+8 keys to choose the layer group where you would like the new object to be created. If you choose to import objects into a specific layer, the object will be placed in the middle layer of the group. For example, if you choose Layer 1 to be the active layer, the object you import will be placed on Z-index "15" in the middle of the Layer 1 group

The following documents where new objects are placed in the Z-index hierarchy if you simply import the object without first defining the working layer. As you can see, most objects are placed at the same level and require the user to manually change the Z-index setting in the object's **Properties** dialog box.

Channels	Layer "50"
Folder	Layer "50"
Line	Layer "50"
Animated Image	Layer "50"
Static Image	Layer "50"
Text Object	Layer "50"
Flash Object	Layer "89"
Hyperlink	Layer "89"
IO Control	Layer "89"

Flash and I.0. Comp Controls are exceptions to Z-index levels. These two object types are always at the top of the Z-index hierarchy no matter what level you try to assign them. This is due to the nature of the controls themselves as they create a separate window in the browser that is above all other content. You will not be able to place any design elements above these two objects to create layered or transparency effects; thus, the Flash and I.O Comp Control objects must have elements stacked beneath them.

To make the best use of these layering, it is important to turn the layer editing function on as you bring elements into the page. For instance, if you want the background images isolated for easy selection, you might bring those objects in while you are editing only Layer "1" (Alt+1). This will place the objects in the middle of the group at Layer "15" and allow you to edit them independent of your other content.

Window Menu

The **Window** menu enables Foreseer Server displays. When active, each of these toggle commands is preceded by a check.

The **Window** menu offers the following Foreseer command:

Tree View - makes the Foreseer Server Tree View, which lists all configured channels hierarchically, the active screen.

Copyright

Foreseer Server Guide – 7.5.800

Publication date 01/2022

EATON CORPORATION - CONFIDENTIAL AND PROPRIETARY NOTICE TO PERSONS RECEIVING THIS DOCUMENT AND/OR TECHNICAL INFORMATION THIS DOCUMENT, INCLUDING THE DRAWING AND INFORMATION CONTAINED THEREON, IS CONFIDENTIAL AND IS THE EXCLUSIVE PROPERTY OF EATON CORPORATION, AND IS MERELY ON LOAN AND SUBJECT TO RECALL BY EATON AT ANY TIME. BY TAKING POSSESSION OF THIS DOCUMENT, THE RECIPIENT ACKNOWLEDGES AND AGREES THAT THIS DOCUMENT CANNOT BE USED IN ANY MANNER ADVERSE TO THE INTERESTS OF EATON, AND THAT NO PORTION OF THIS DOCUMENT MAY BE COPIED OR OTHERWISE REPRODUCED WITHOUT THE PRIOR WRITTEN CONSENT OF EATON. IN THE CASE OF CONFLICTING CONTRACTUAL PROVISIONS, THIS NOTICE SHALL GOVERN THE STATUS OF THIS DOCUMENT.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation’s (“Eaton”) experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein.